BigFix Insights for Vulnerability Remediation

Implementation Guide

Special notice

Before using this information and the product it supports, read the information in Notices.

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. BigFix Insights for Vulnerability Remediation

Use this section to become familiar with BigFix Insights for Vulnerability Remediation infrastructure and key concepts necessary to understand how it works.

BigFix Insights for Vulnerability Remediation integrates BigFix with sources of vulnerability data. The purpose is to guide BigFix users on how to apply the best patch and configuration settings to remediate discovered vulnerabilities, and thus reduce risk and improve security.

BigFix Insights for Vulnerability Remediation uses advanced correlation algorithms to aggregate and process the vulnerability data with information from BigFix to drive analytics reports. The output of the analytics facilitates remediation through the Baseline Creation Wizard by recommending the latest available patches for the discovered vulnerabilities.

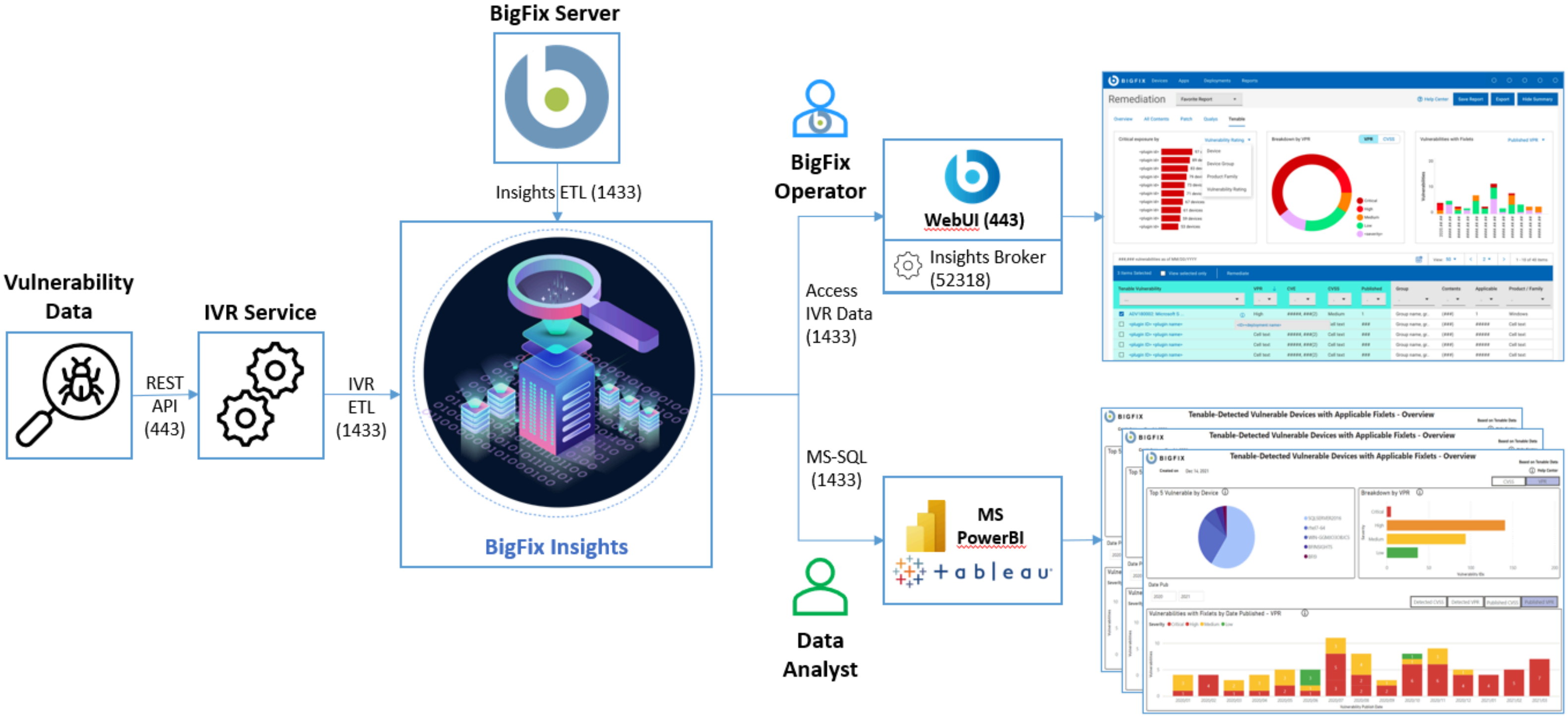
IVR data is available in:

- WebUI IVR app - it is required to enable WebUI to access IVR data through Insights. For more information on installing IVR app, see Setting up IVR App.
- BI Tools for Data Analysis - existing IVR reports in PowerBI and Tableau. Refer to the link to find out more about IVR reports.

IVR limitations:

- Only one source of vulnerability data for automatic ingestion is supported for a given BigFix Insights instance
- One BigFix WebUI instance can manage only one BigFix Insights database. This limitation means that you cannot simultaneously connect or manage multiple instances of BigFix Insights through one WebUI instance.

Figure 1. Architecture overview of BigFix Insights for Vulnerability Remediation



Chapter 2. System requirements

Learn more about the prerequisites and system requirements for BigFix Insights for Vulnerability Remediation (IVR) service.

Table 1. Prerequisites and system requirements for IVR service

Hardware requirements	
CPU	minimum 2 cores (recommended 4)
RAM	On top of host OS requirements: • < 1M Findings from Vulnerability Management Product = 16GB • < 2M Findings from Vulnerability Management Product = 32GB • < 3M Findings from Vulnerability Management Product = 48GB • < 4M Findings from Vulnerability Management Product = 64GB
Disc space	• < 1M Findings from Vulnerability Management Product = 4GB - 8GB preferred • < 2M Findings from Vulnerability Management Product = 8GB - 12GB preferred • < 3M Findings from Vulnerability Management Product = 12GB - 16GB preferred • < 4M Findings from Vulnerability Management Product = 16GB - 20GB preferred
Execution Time	The overall run time of data synchronization and processing depends on: • CPU Speed • Number of findings • Number of assets in insights • Number of patch sites loaded within the BFE environment • API latency • Conflicting workloads on IVR machine
Software requirements	

Table 1. Prerequisites and system requirements for IVR service (continued)

BigFix Component Requirements	• BigFix Insights WebUI App (v6) (minimum)
Prerequisites	• Microsoft VC++ Redistributable package 2012 https://www.microsoft.com/en-in/download/details.aspx?id=30679 • Microsoft® ODBC Driver 17 for SQL Server® https://www.microsoft.com/en-us/download/details.aspx?id=56567 **Note:** The Fixlet will attempt to deploy the pre-requisites automatically.
Operating system	• Microsoft Windows 2016 • Microsoft Windows 2019
Supported BigFix versions	• Windows - based BigFix Server, Version 10 **Note:** BigFix Insights for Vulnerability Remediation does not currently support non-Windows-based BigFix Server environments.
BigFix License Requirements	• BigFix Lifecycle • BigFix Compliance • BigFix Remediate
Supported Vulnerability Management Platforms	• Qualys VMDR v2 REST API: https://www.qualys.com/docs/qualys-api-vm-pc-user-guide.pdf • Tenable.SC versions from 5.17 up to 6.0.0. • Tenable.IO

Table 1. Prerequisites and system requirements for IVR service (continued)

	Note: It is required to use **Administrator** user role within Tenable to enable the generation of API keys that are used by IVR to maintain the interface with Tenable.
BI tool	• Power BI Desktop/Server, 2021 + (Rec. May 2021) **Note:** Microsoft offers two distinct products called Power BI desktop. Use the one that is optimized for Power BI Report Server: https://www.microsoft.com/en-us/download/details.aspx?id=56723 • Tableau Desktop/Server, 2020.4 +
Network requirements	• Connectivity to Vulnerability Management API Server URL (port 443 by default) • Connectivity to BigFix Insights SQL database (port 1433 by default) **Note:** IVR now supports proxy-based connectivity. Refer to the link for more information. • By default WebUI IVR app listens on port 52318. It can be changed in the WebUI application configuration file with `_WebUIAppEnv_INSIGHT_BROKER_PORT` setting.

Table 1. Prerequisites and system requirements for IVR service (continued)

System limitations	• Only one source of vulnerability data for automatic ingestion is supported for a given BigFix Insights instance • A single BigFix WebUI instance can manage only one BigFix Insights database.

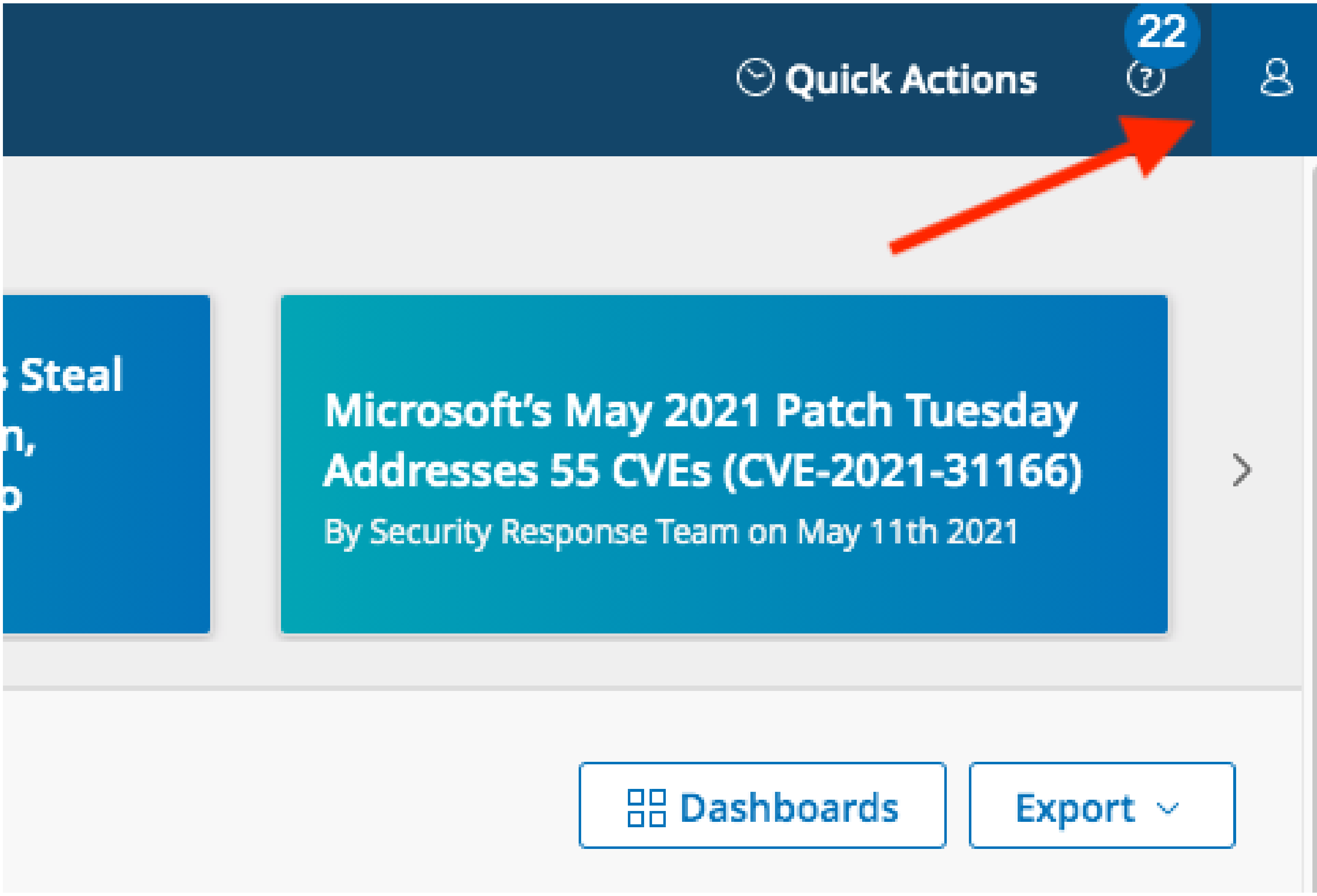
API requirements for Tenable.io

To ensure that IVR can retrieve the essential vulnerability data from Tenable, it is necessary to meet the following requirements:

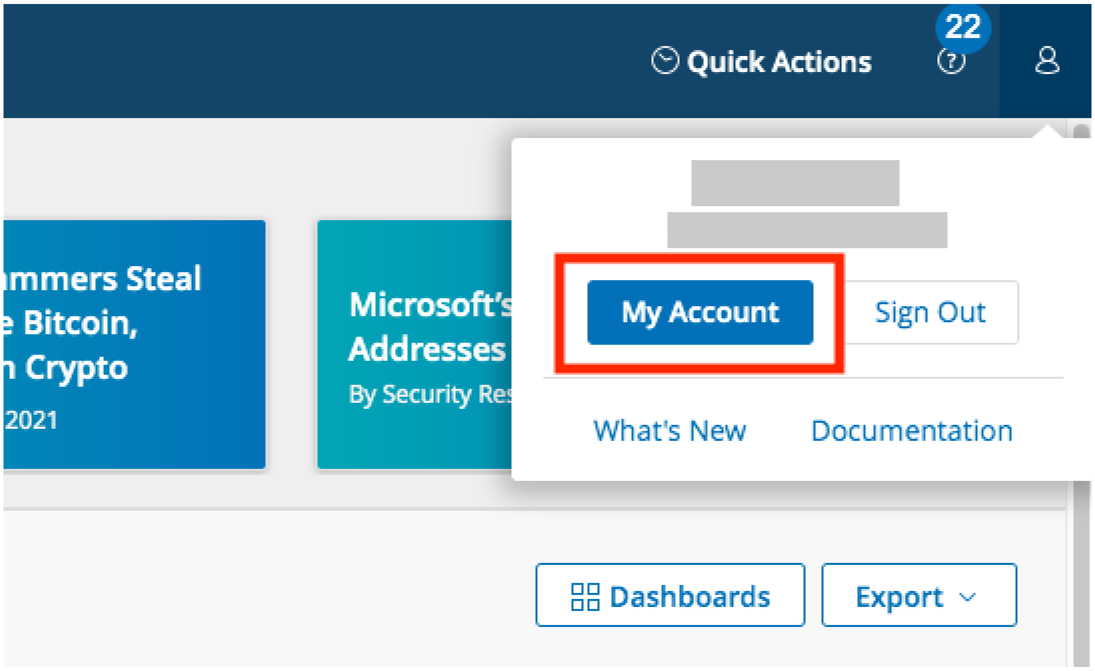
- User with **Administrator** user role within Tenable
- **All Assets** set to **Can View**. For more information, see Tenable Permissions.

To generate User's API keys:

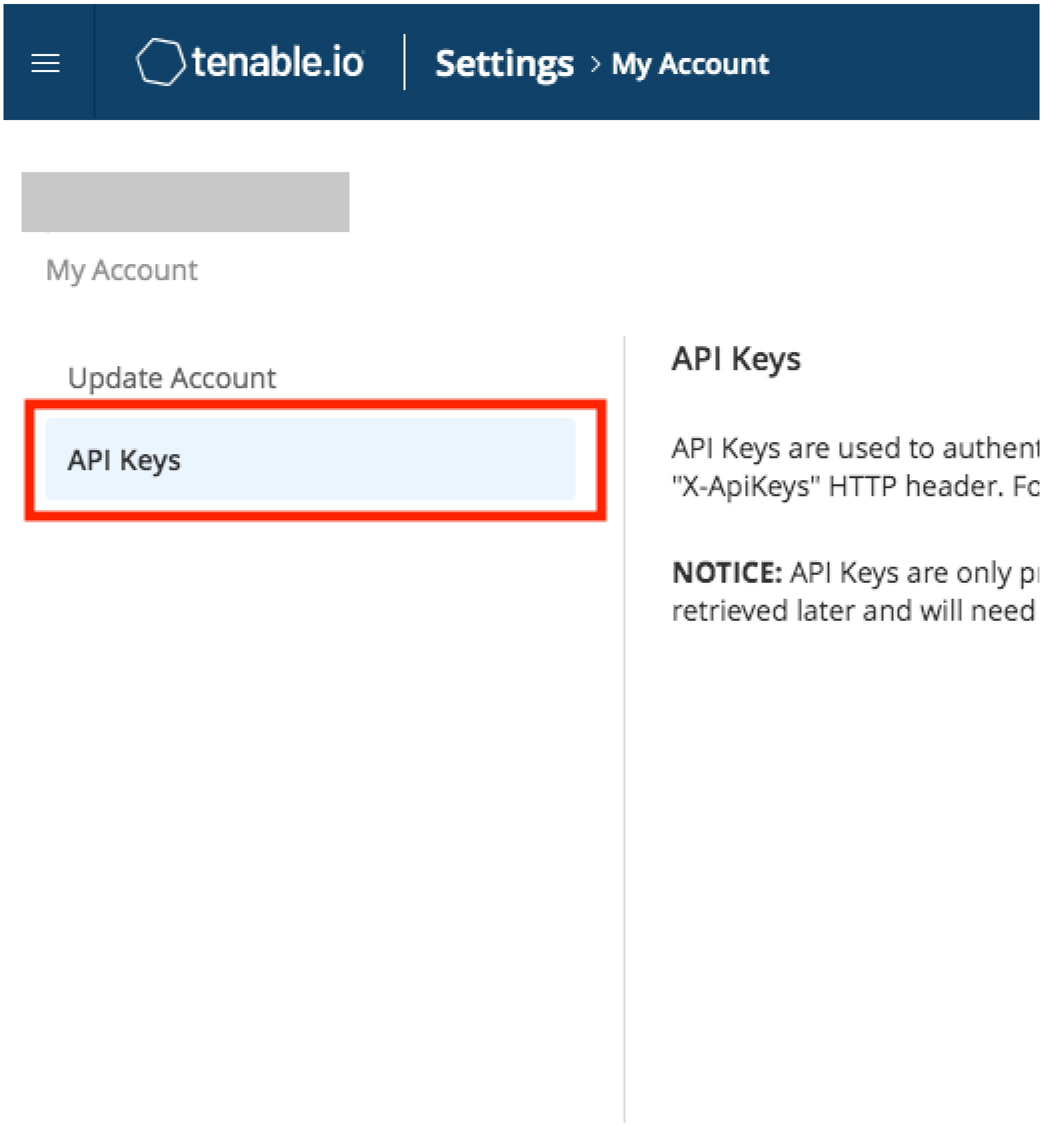
1. In the Tenable.io web user interface, click the button on the top right corner of the header.


Quick Actions
22
Steal
n,
o
Microsoft's May 2021 Patch Tuesday Addresses 55 CVEs (CVE-2021-31166)
By Security Response Team on May 11th 2021
Dashboards
Export

2. Click **My account** button. The user account menu appears.



3. Select **API Keys** from the left-hand navigation.

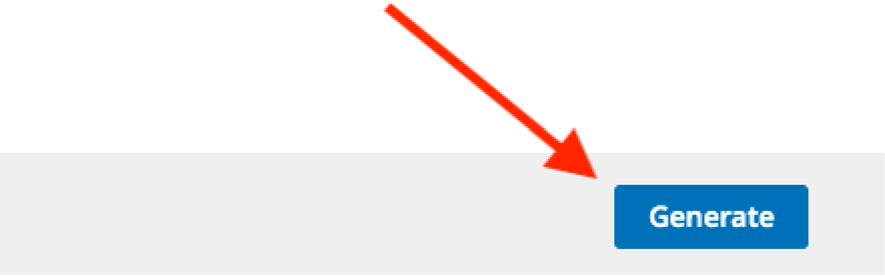


API Keys

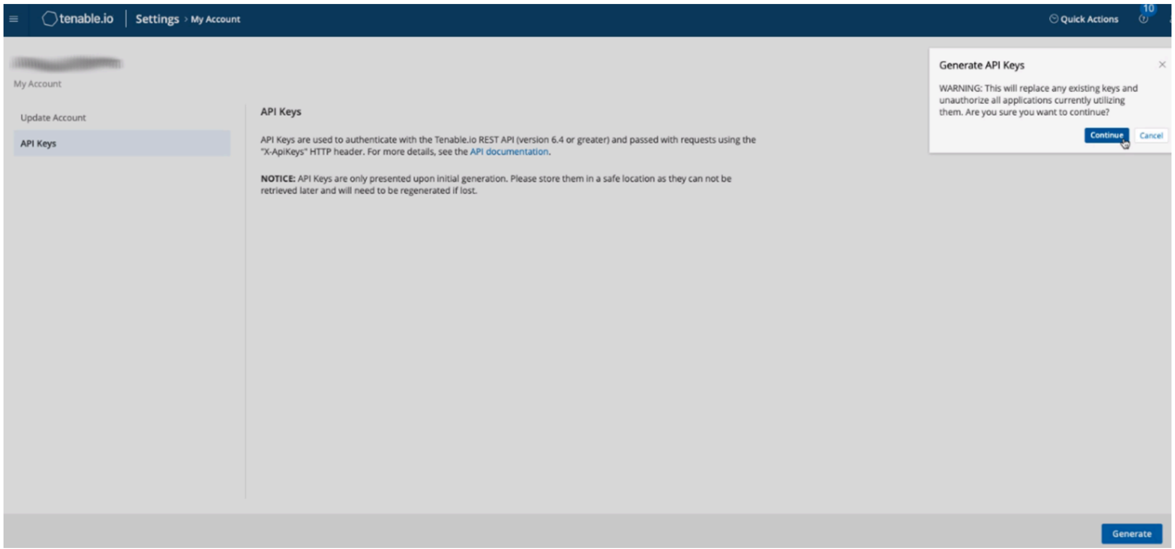
API Keys are used to authent
"X-ApiKeys" HTTP header. Fo

NOTICE: API Keys are only p
retrieved later and will need

4. Click the **Generate** button in the lower right part of the browser.



5. Acknowledge the warning by clicking **Continue** in the pop-up box.



[redacted]

My Account

Update Account

API Keys

API Keys

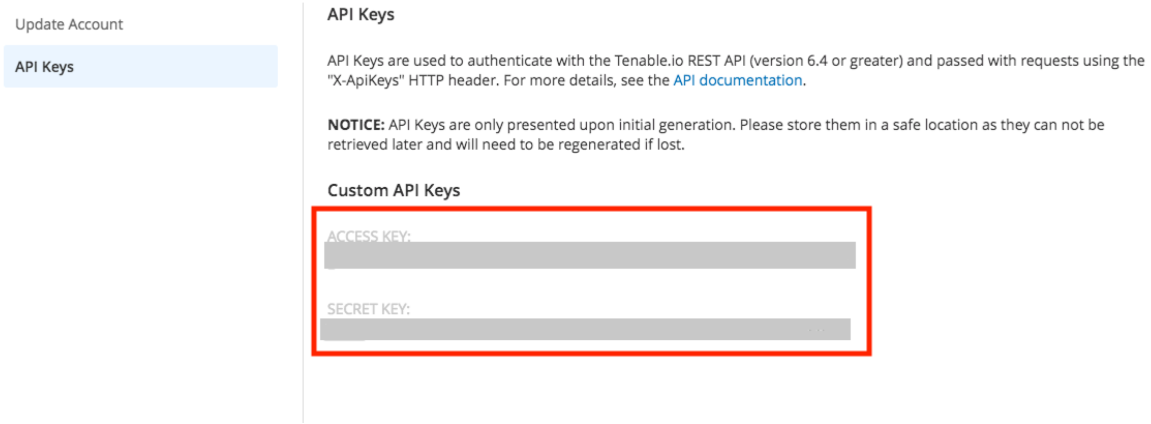
API Keys are used to authenticate with the Tenable.io REST API (version 6.4 or greater) and passed with requests using the "X-ApiKeys" HTTP header. For more details, see the API documentation.

NOTICE: API Keys are only presented upon initial generation. Please store them in a safe location as they can not be retrieved later and will need to be regenerated if lost.

Generate API Keys

WARNING: This will replace any existing keys and unauthorize all applications currently utilizing them. Are you sure you want to continue?

6. Tenable.io generates new access key and secret key. Copy the two generated keys and paste into the IVR configuration page to enable the interface. **Be sure to copy access and secret keys to a safe location as keys are displayed only once**. After the tab is closed, API keys cannot be retrieved from Tenable.io.



Update Account

API Keys

API Keys

API Keys are used to authenticate with the Tenable.io REST API (version 6.4 or greater) and passed with requests using the "X-ApiKeys" HTTP header. For more details, see the API documentation.

NOTICE: API Keys are only presented upon initial generation. Please store them in a safe location as they can not be retrieved later and will need to be regenerated if lost.

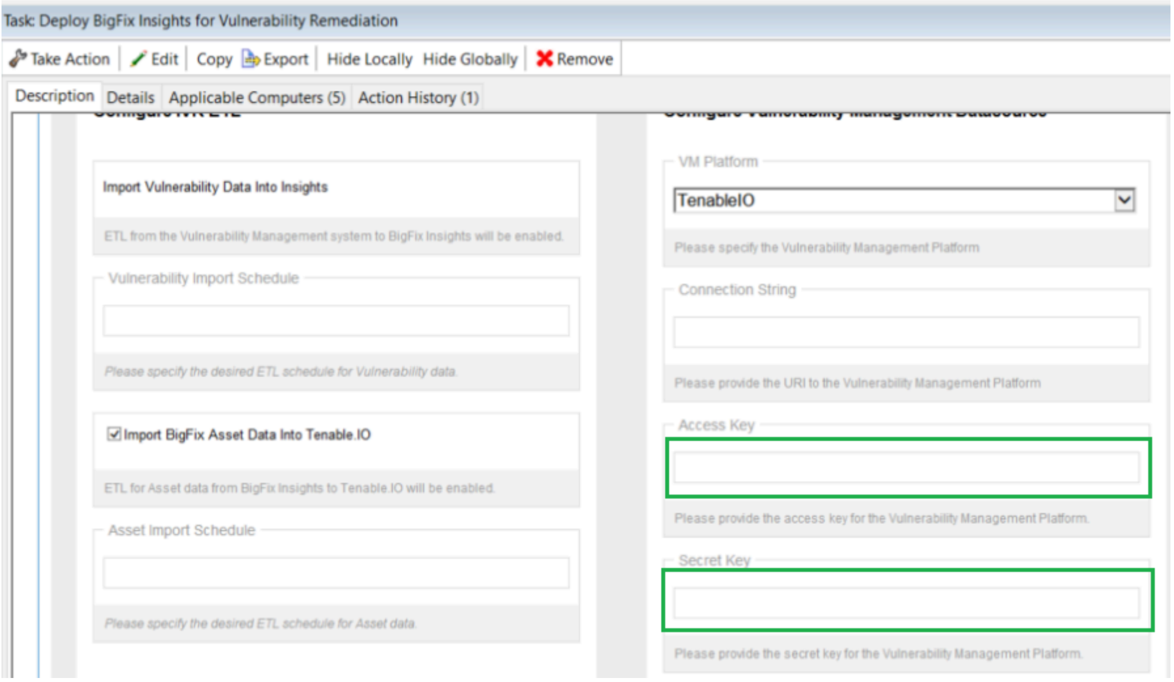
Custom API Keys

ACCESS KEY: [redacted]

SECRET KEY: [redacted]

Once the API keys are generated, you can proceed with the Deployment process.

In the Deployment Fixlet, you will need to provide the Access Key and the Secret Key.



Import Vulnerability Data Into Insights

ETL from the Vulnerability Management system to BigFix Insights will be enabled.

Vulnerability Import Schedule

Please specify the desired ETL schedule for Vulnerability data.

☑ Import BigFix Asset Data Into Tenable.IO

ETL for Asset data from BigFix Insights to Tenable.IO will be enabled.

Asset Import Schedule

Please specify the desired ETL schedule for Asset data.

VM Platform: TenableIO

Please specify the Vulnerability Management Platform

Connection String

Please provide the URI to the Vulnerability Management Platform

Access Key

Please provide the access key for the Vulnerability Management Platform.

Secret Key

Please provide the secret key for the Vulnerability Management Platform.

Refer to this page for more information about User Roles and Permissions:https://docs.tenable.com/tenableio/Content/Settings/UserRoles.htm

With the API keys generated, you can validate API credentials by using below curl commands:

a. Get Vuln Export UUID:

```
curl --request POST --url https://cloud.tenable.com/vulns/export --header "Accept: application/json" --header "Content-Type: application/json" --header "X-ApiKeys: accessKey=redactedaccesskey; secretKey=redactedsecretkey"
```

b. Get Vuln Export Status for given UUID:

```
curl --request GET --url https://cloud.tenable.com/vulns/export/21a70c98-8e8d-4b64-b7e0-4c57a245126f/status --header "Accept: application/json" --header "Content-Type: application/json" --header "X-ApiKeys: accessKey=redactedaccesskey; secretKey=redactedsecretkey"
```

c. Get Chunk 1 of vuln data for given UUID:

```
curl --request GET --url https://cloud.tenable.com/vulns/export/21a70c98-8e8d-4b64-b7e0-4c57a245126f/chunks/1 --header "Accept: application/octet-stream" --header "X-ApiKeys: accessKey=redactedaccesskey; secretKey=redactedsecretkey"
```

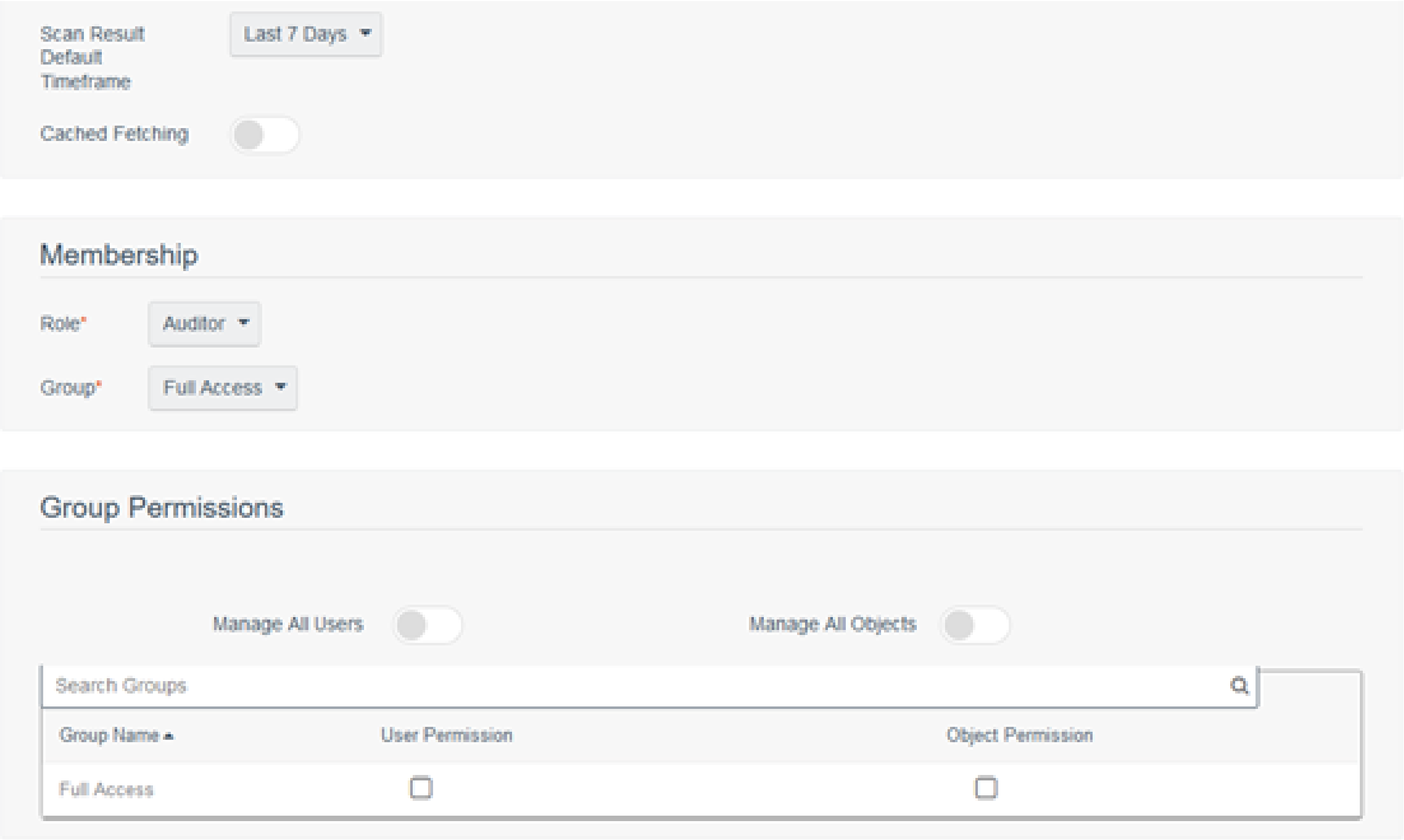
In each example above, replace ‘redactedaccesskey’ and ‘redactedsecretkey’ with the same API keys/ credentials as those being used for the integration. Also, for API calls 2 and 3, replace the example UUID in the request URL (21a70c98-8e8d-4b64-b7e0-4c57a245126f) with the UUID value returned from API call 1.

API requirements for Tenable.sc

The IVR server requires a Tenable user account. A user leveraged to Tenable.sc IVR adapter needs compatible machines within the environment.

The Tenable account utilized for IVR should be assigned the default full access group, and auditor role permissions. This provides the account access needed to complete the dataflow. Additionally, the user can be defined using custom access permissions to limit the scope of assets retrieved by IVR. A group within Tenable can be limited by both the viewable hosts and the repositories. In general, the role of auditor should be leveraged as well, to follow the principle of least privileged. The IVR dataflow retrieves information only when the account has granted visibility to receive.

Here is how the “Create User” page, Membership section should look like the new user is created:



Scan Result Default Timeframe: Last 7 Days

Cached Fetching: ○

Membership

Role*: Auditor

Group*: Full Access

Group Permissions

Manage All Users: ○

Manage All Objects: ○

Search Groups

Group Name ▲	User Permission	Object Permission
Full Access	□	□

Tenable impact statement

IVR uses the pytenable library (developed by Tenable). IVR leverages a default batch size of 1000, which is conservative and is prescribed by Tenable. With the default settings, the Tenable.sc server should not see a noticeable impact when the IVR adapter is running.

API requirements for Qualys

Qualys API requirements

The Qualys API enforces limits on the API calls a customer can make based on their subscription settings. The limits apply to the use of all Qualys APIs except “session” V2 API (session login/logout). Default API control settings are provided by the service. Note these settings may be customized per subscription by Qualys Support.

For more details, refer to the link: https://www.qualys.com/docs/qualys-api-limits.pdf.

To estimate the number of API calls, use the below formula:

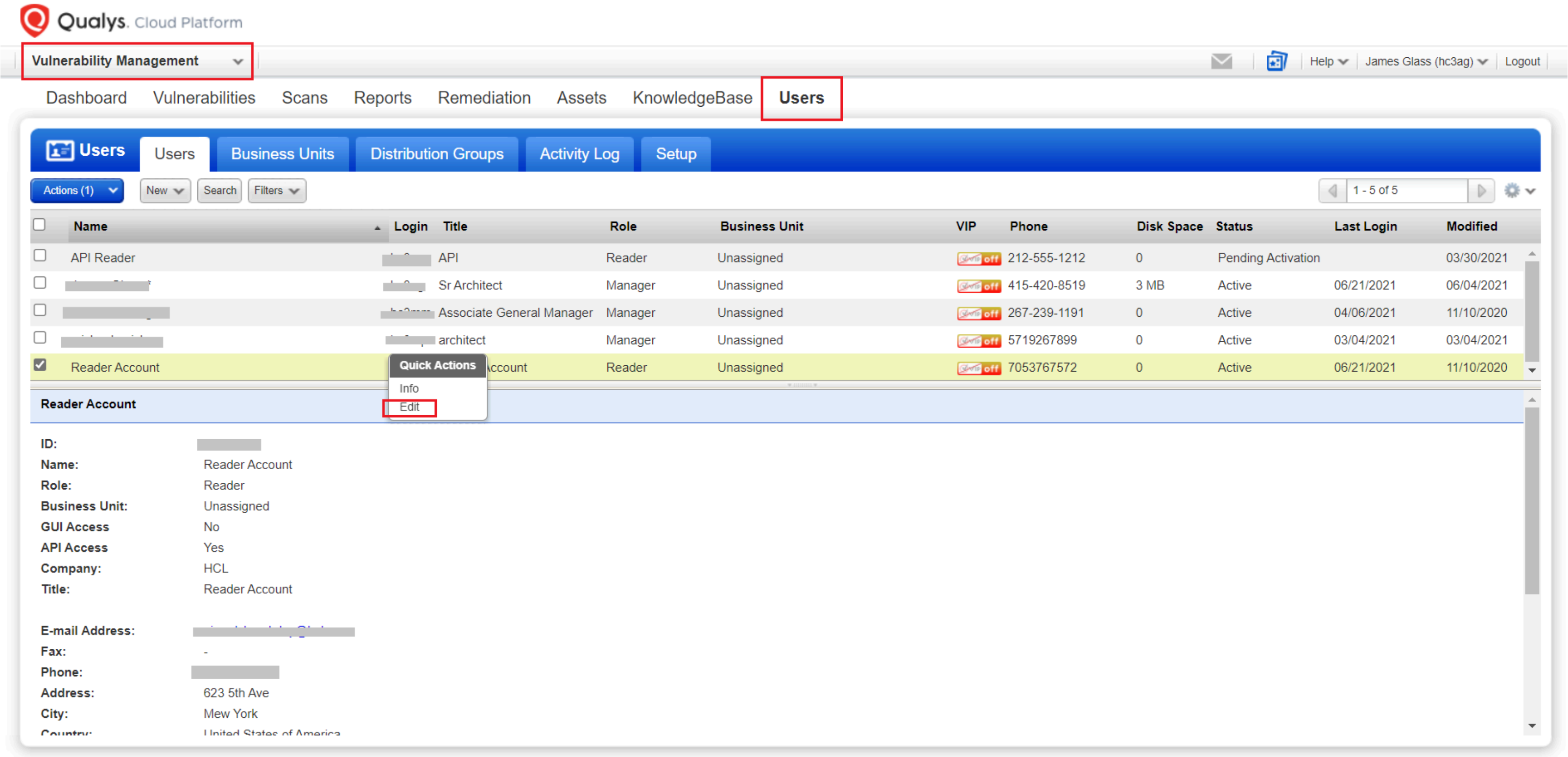
```
Total number of API calls = (number of devices / batch size ) + (number of unique vulnerabilities / 350)
```

where;

- `batch size` - configurable parameter that describes the maximum number of devices which can be fetched in a single API call
- `number of devices` - number of available devices in the scanned network
- `number of unique vulnerabilities` - number of unique vulnerabilities discovered in the scanned network
- `350` - maximum number of vulnerabilities that can be fetched in a single API call into the Qualys Knowledge Base API.

Qualys API User requirements

It is recommended to use 'Reader' user role. To edit user account, select **Users** tab in the **Vulnerability Management** dashboard. Hover the cursor over the **Login** and click **Edit**.

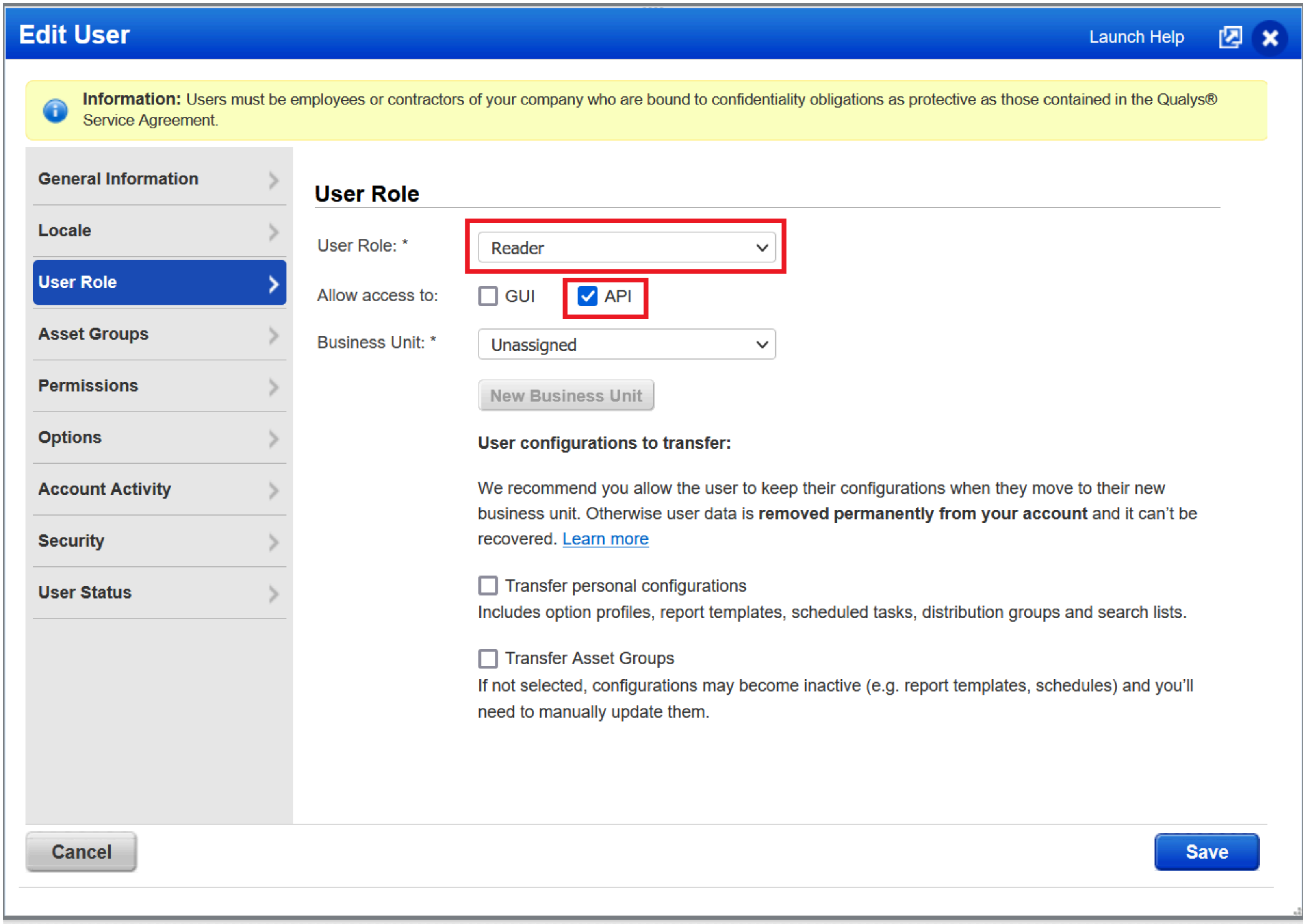


☐	Name	Login	Title	Role	Business Unit	VIP	Phone	Disk Space	Status	Last Login	Modified
☐	API Reader	[redacted]	API	Reader	Unassigned	off	212-555-1212	0	Pending Activation		03/30/2021
☐	[redacted]	[redacted]	Sr Architect	Manager	Unassigned	off	415-420-8519	3 MB	Active	06/21/2021	06/04/2021
☐	[redacted]	[redacted]	Associate General Manager	Manager	Unassigned	off	267-239-1191	0	Active	04/06/2021	11/10/2020
☐	[redacted]	[redacted]	architect	Manager	Unassigned	off	5719267899	0	Active	03/04/2021	03/04/2021
☑	Reader Account		ccount	Reader	Unassigned	off	7053767572	0	Active	06/21/2021	11/10/2020

Reader Account

ID:	[redacted]
Name:	Reader Account
Role:	Reader
Business Unit:	Unassigned
GUI Access	No
API Access	Yes
Company:	HCL
Title:	Reader Account
E-mail Address:	[redacted]
Fax:	-
Phone:	[redacted]
Address:	623 5th Ave
City:	Mew York
Country:	United States of America

In the **User Role** tab, select **Reader** as a user role and **Allow access to API**.



Information: Users must be employees or contractors of your company who are bound to confidentiality obligations as protective as those contained in the Qualys® Service Agreement.

User Role

User Role: * Reader

Allow access to: □ GUI ☑ API

Business Unit: * Unassigned

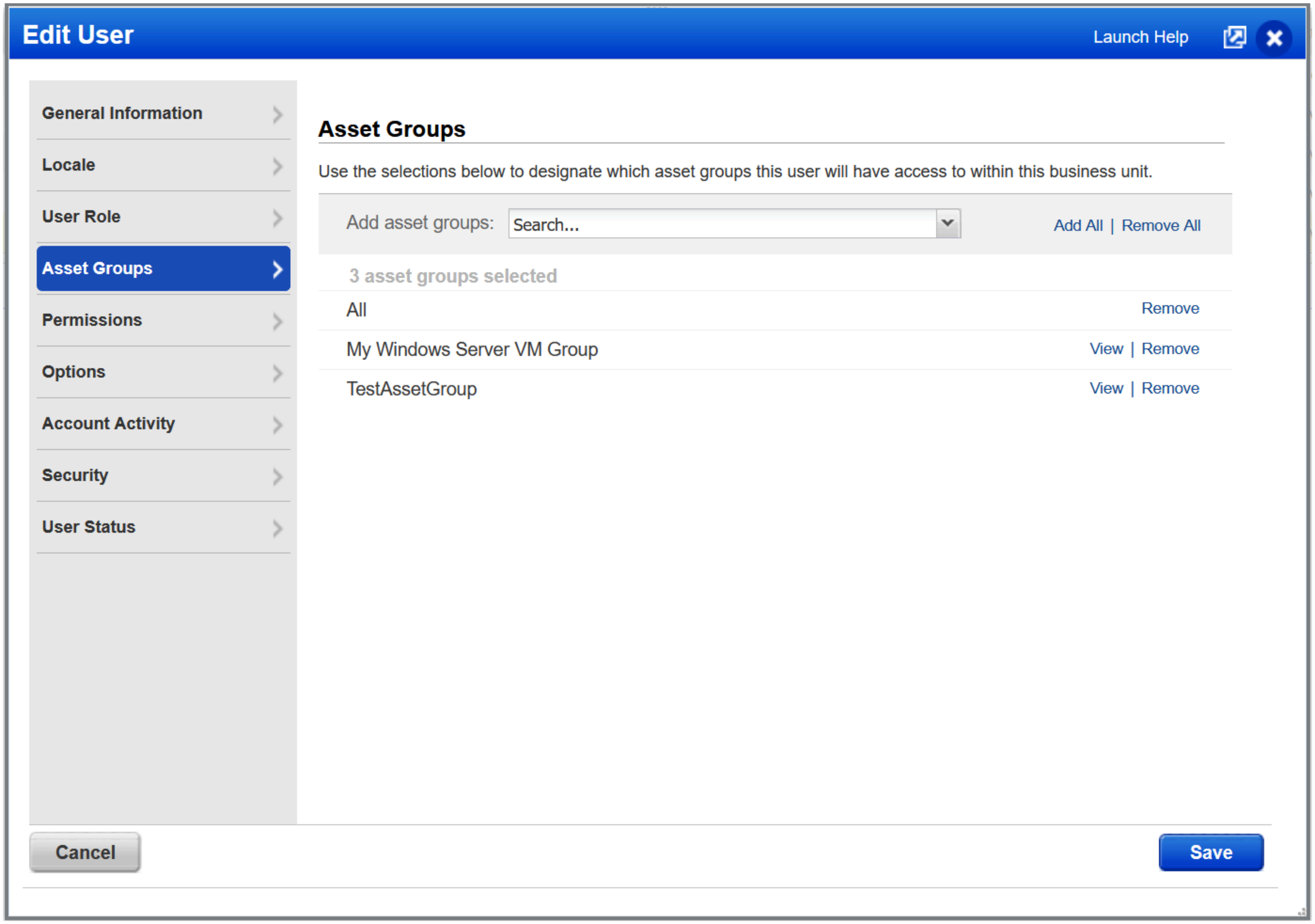
User configurations to transfer:

We recommend you allow the user to keep their configurations when they move to their new business unit. Otherwise user data is **removed permanently from your account** and it can't be recovered. Learn more

□ Transfer personal configurations
Includes option profiles, report templates, scheduled tasks, distribution groups and search lists.

□ Transfer Asset Groups
If not selected, configurations may become inactive (e.g. report templates, schedules) and you'll need to manually update them.

In the **Asset Groups** tab, you can select asset groups that you wish to have access to.



Asset Groups

Use the selections below to designate which asset groups this user will have access to within this business unit.

Add asset groups: Search...

3 asset groups selected

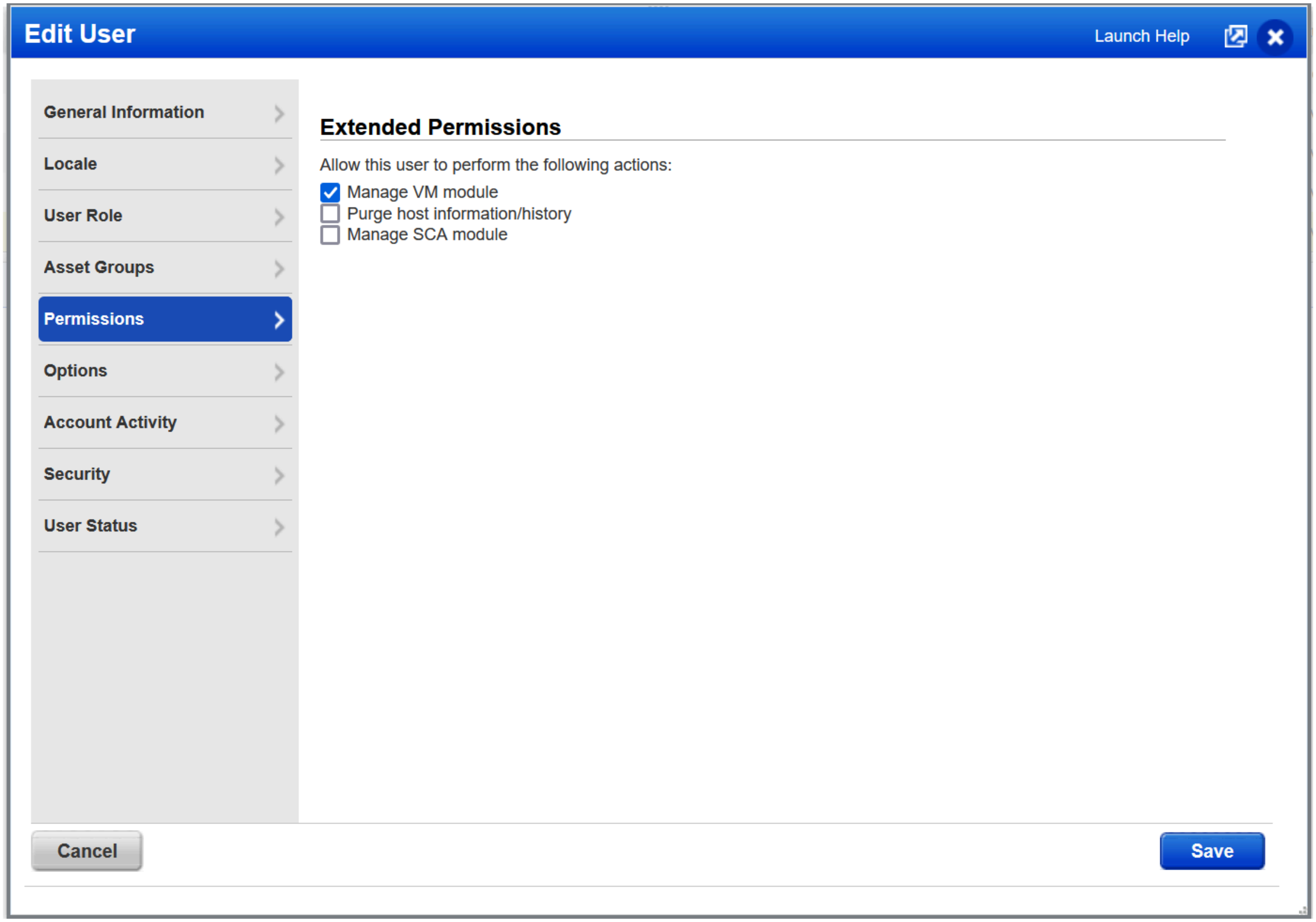
All

My Windows Server VM Group

TestAssetGroup

For more information on how to assign asset groups to the user, refer to the link.

In the **Permissions** tab select **Manage VM module**.



Extended Permissions

Allow this user to perform the following actions:

☑ Manage VM module
□ Purge host information/history
□ Manage SCA module

Refer to the link to find more information on User roles and permissions.

Chapter 3. Deployment and configuration

This module provides the steps to deploy and configure the BigFix Insights for Vulnerability Remediation solution for:

Tenable.io

Tenable.sc

Qualys

Refer to the link to learn more about other Fixlets and Tasks available for BigFix Insights for Vulnerability Remediation solution.

Deployment and configuration for Tenable.io

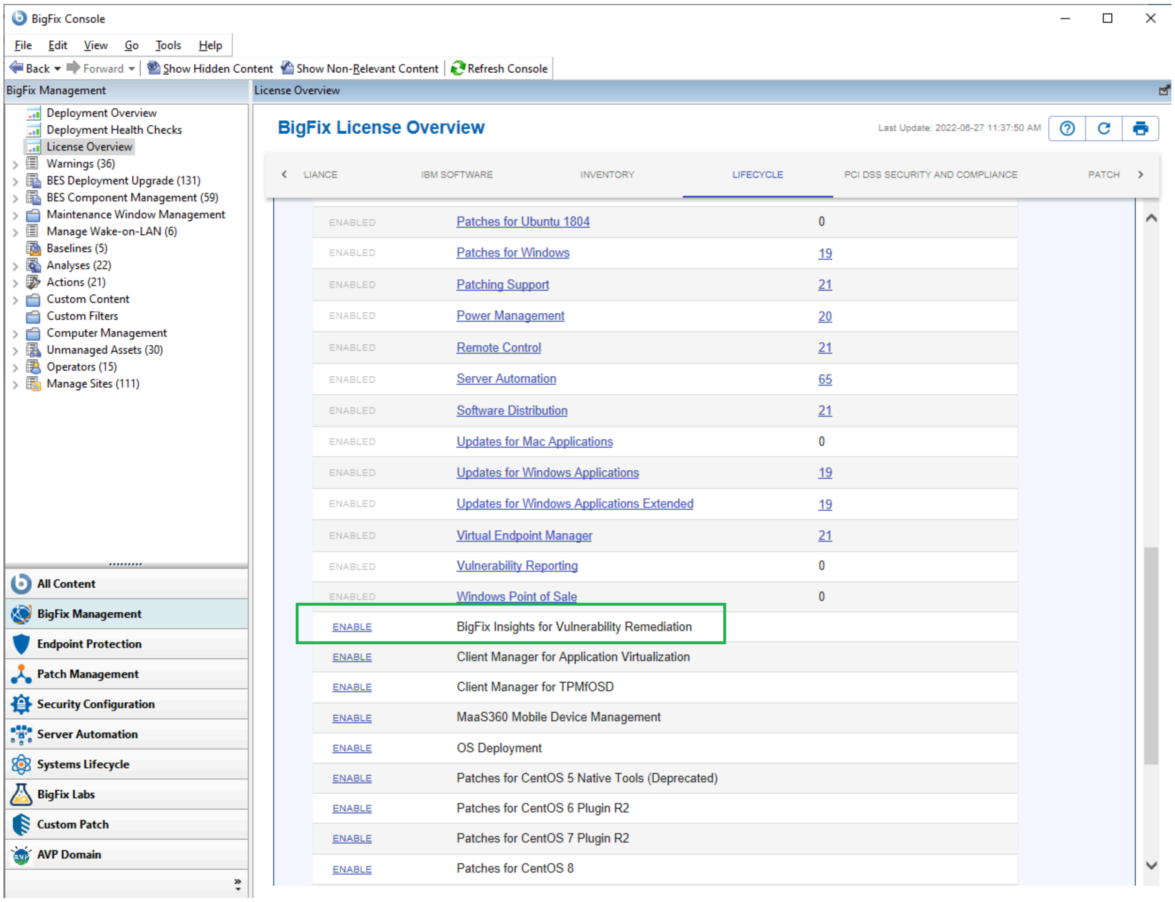
This module provides the steps to deploy and configure the BigFix Insights for Vulnerability Remediation solution.

To install and configure BigFix Insights for Vulnerability Remediation service, perform below steps:

Note: To use the latest release build, uninstall the old version.

1. Enable a content site.

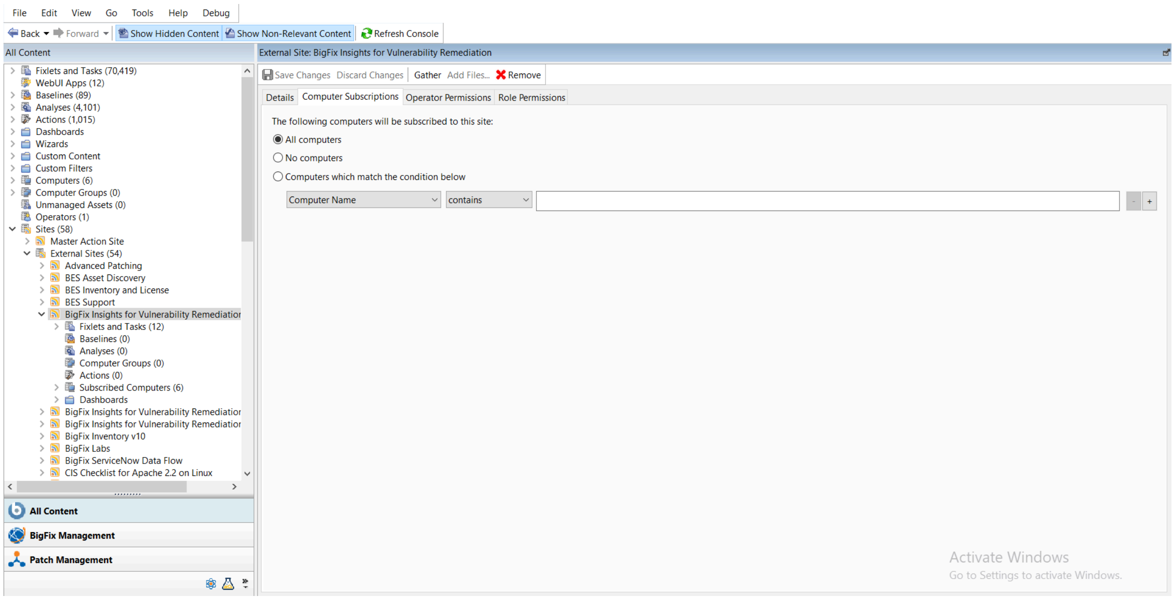
   Navigate to BigFix License Overview Dashboard. In **Compliance/Lifecycle** panel, click **Enable BigFix Insights for Vulnerability Remediation** Fixlet to gather the required content.



ENABLED	Patches for Ubuntu 1804	0
ENABLED	Patches for Windows	19
ENABLED	Patching Support	21
ENABLED	Power Management	20
ENABLED	Remote Control	21
ENABLED	Server Automation	65
ENABLED	Software Distribution	21
ENABLED	Updates for Mac Applications	0
ENABLED	Updates for Windows Applications	19
ENABLED	Updates for Windows Applications Extended	19
ENABLED	Virtual Endpoint Manager	21
ENABLED	Vulnerability Reporting	0
ENABLED	Windows Point of Sale	0
ENABLE	BigFix Insights for Vulnerability Remediation	
ENABLE	Client Manager for Application Virtualization	
ENABLE	Client Manager for TPMfOSD	
ENABLE	MaaS360 Mobile Device Management	
ENABLE	OS Deployment	
ENABLE	Patches for CentOS 5 Native Tools (Deprecated)	
ENABLE	Patches for CentOS 6 Plugin R2	
ENABLE	Patches for CentOS 7 Plugin R2	
ENABLE	Patches for CentOS 8	

Note: Refer to the following link for more information about **License Overview dashboard**.

2. Subscribe computers to the site. It is recommended to subscribe to All computers. For more information on **Computer Subscriptions Tab** refer to the link.


File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (70,419)
WebUI Apps (12)
Baselines (89)
Analyses (4,101)
Actions (1,015)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (6)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (58)
Master Action Site
External Sites (54)
Advanced Patching
BES Asset Discovery
BES Inventory and License
BES Support
BigFix Insights for Vulnerability Remediation
Fixlets and Tasks (12)
Baselines (0)
Analyses (0)
Computer Groups (0)
Actions (0)
Subscribed Computers (6)
Dashboards
BigFix Insights for Vulnerability Remediation
BigFix Insights for Vulnerability Remediation
BigFix Inventory v10
BigFix Labs
BigFix ServiceNow Data Flow
CIS Checklist for Apache 2.2 on Linux
All Content
BigFix Management
Patch Management
External Site: BigFix Insights for Vulnerability Remediation
Save Changes Discard Changes Gather Add Files... Remove
Details Computer Subscriptions Operator Permissions Role Permissions
Activate Windows
Go to Settings to activate Windows.

The following computers will be subscribed to this site:

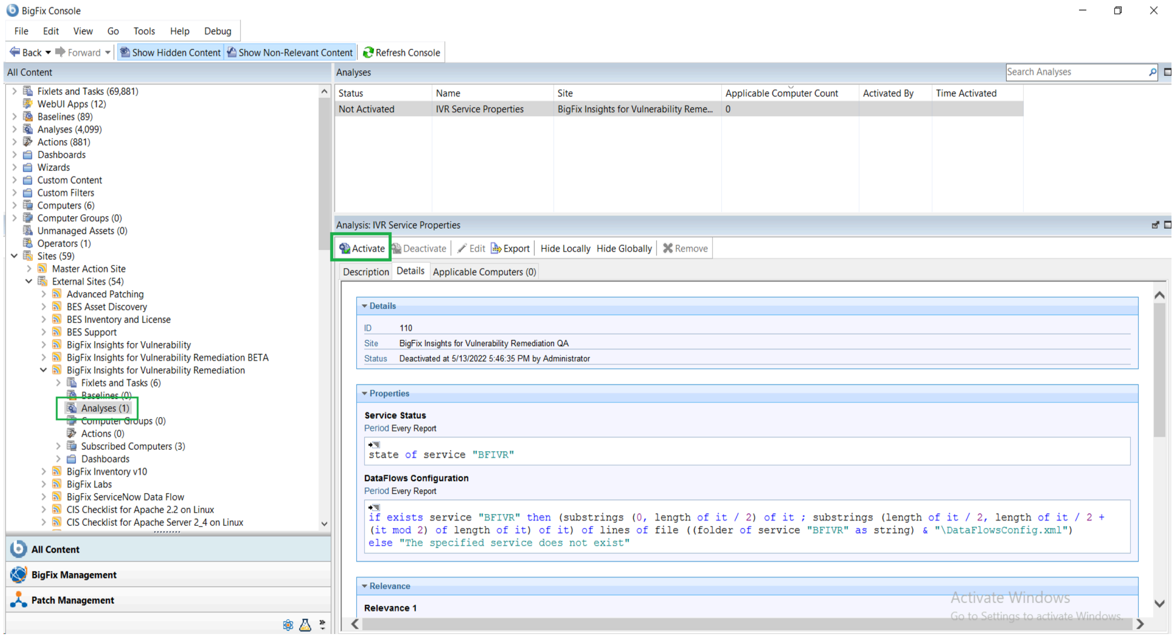
● All computers

○ No computers

○ Computers which match the condition below

Computer Name | contains

3. Activate the analysis.


BigFix Console
File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (69,881)
WebUI Apps (12)
Baselines (89)
Analyses (4,099)
Actions (881)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (6)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (59)
Master Action Site
External Sites (54)
Advanced Patching
BES Asset Discovery
BES Inventory and License
BES Support
BigFix Insights for Vulnerability
BigFix Insights for Vulnerability Remediation BETA
BigFix Insights for Vulnerability Remediation
Fixlets and Tasks (6)
Baselines (0)
Analyses (1)
Computer Groups (0)
Actions (0)
Subscribed Computers (3)
Dashboards
BigFix Inventory v10
BigFix Labs
BigFix ServiceNow Data Flow
CIS Checklist for Apache 2.2 on Linux
CIS Checklist for Apache Server 2_4 on Linux
All Content
BigFix Management
Patch Management
Analyses
Search Analyses
Analysis: IVR Service Properties
Activate Deactivate Edit Export Hide Locally Hide Globally Remove
Description Details Applicable Computers (0)
Details
Properties
Relevance
Relevance 1
Activate Windows
Go to Settings to activate Windows.

Status	Name	Site	Applicable Computer Count	Activated By	Time Activated
Not Activated	IVR Service Properties	BigFix Insights for Vulnerability Reme...	0		

ID 110

Site BigFix Insights for Vulnerability Remediation QA

Status Deactivated at 5/13/2022 5:46:35 PM by Administrator

Service Status

Period Every Report

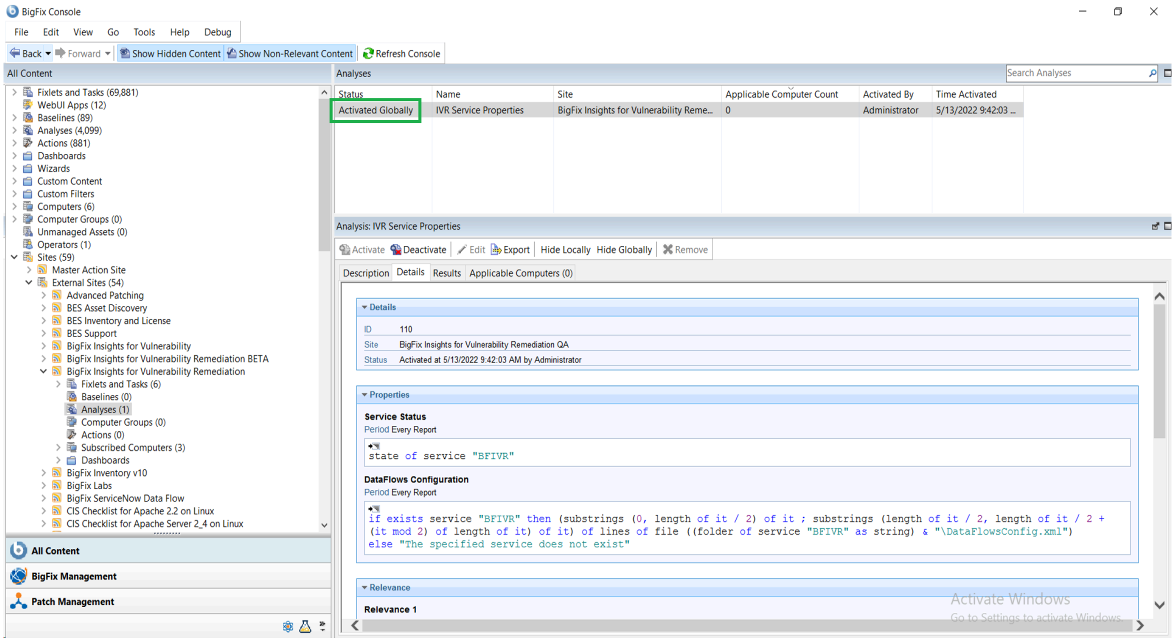
```
state of service "BFIVR"
```

DataFlows Configuration

Period Every Report

```
if exists service "BFIVR" then (substrings (0, length of it / 2) of it ; substrings (length of it / 2, length of it / 2 +
(it mod 2) of length of it) of it) of lines of file ((folder of service "BFIVR" as string) & "\DataFlowsConfig.xml")
else "The specified service does not exist"
```

Status of the analysis should be **Activated Globally**.


BigFix Console
File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (69,881)
WebUI Apps (12)
Baselines (89)
Analyses (4,099)
Actions (881)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (6)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (59)
Master Action Site
External Sites (54)
Advanced Patching
BES Asset Discovery
BES Inventory and License
BES Support
BigFix Insights for Vulnerability
BigFix Insights for Vulnerability Remediation BETA
BigFix Insights for Vulnerability Remediation
Fixlets and Tasks (6)
Baselines (0)
Analyses (1)
Computer Groups (0)
Actions (0)
Subscribed Computers (3)
Dashboards
BigFix Inventory v10
BigFix Labs
BigFix ServiceNow Data Flow
CIS Checklist for Apache 2.2 on Linux
CIS Checklist for Apache Server 2_4 on Linux
All Content
BigFix Management
Patch Management
Analyses
Search Analyses
Analysis: IVR Service Properties
Activate Deactivate Edit Export Hide Locally Hide Globally Remove
Description Details Results Applicable Computers (0)
Activate Windows
Go to Settings to activate Windows.

Status	Name	Site	Applicable Computer Count	Activated By	Time Activated
Activated Globally	IVR Service Properties	BigFix Insights for Vulnerability Reme...	0	Administrator	5/13/2022 9:42:03 ...

Details

ID 110
Site BigFix Insights for Vulnerability Remediation QA
Status Activated at 5/13/2022 9:42:03 AM by Administrator

Properties

Service Status
Period Every Report

```
state of service "BFIVR"
```

DataFlows Configuration
Period Every Report

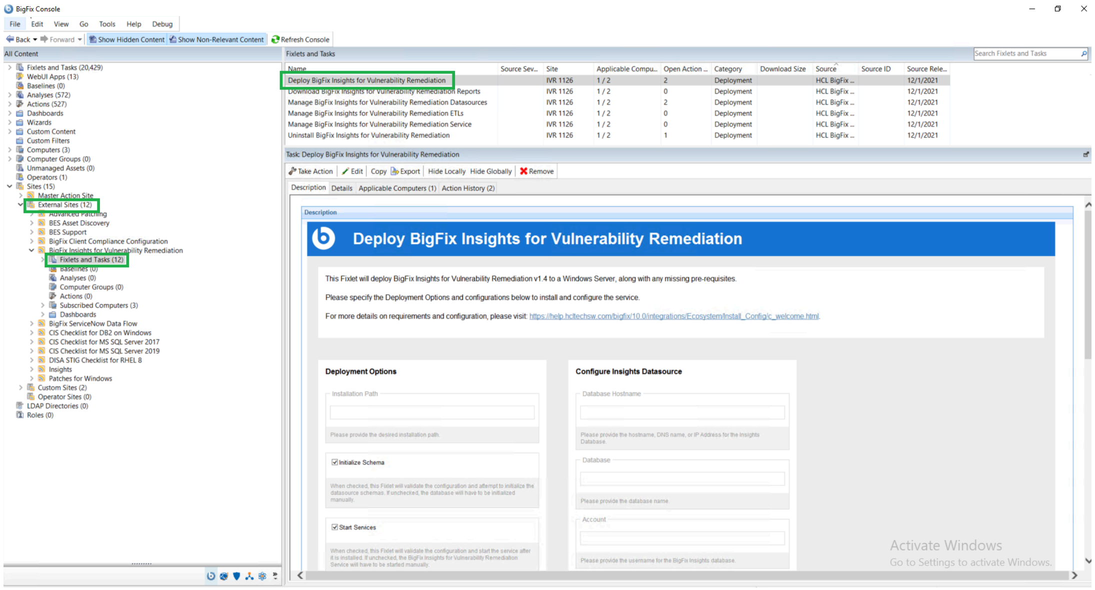
```
if exists service "BFIVR" then (substrings (0, length of it / 2) of it ; substrings (length of it / 2, length of it / 2 +
(it mod 2) of length of it) of it) of lines of file ((folder of service "BFIVR" as string) & "\DataFlowsConfig.xml")
else "The specified service does not exist"
```

Relevance

Relevance 1

Note: Refer to the link to learn more about **Computer Subscriptions** Tab.

4. Deploy the solution to the target server.
   a. Click **Deploy Insights for Vulnerability Remediation** Fixlet in the **BigFix Insights for Vulnerability Remediation** external sites.


BigFix Console
File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (20,429)
WebUI Apps (13)
Baselines (0)
Analyses (572)
Actions (527)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (3)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (15)
Master Action Site
External Sites (12)
Advanced Patching
BES Asset Discovery
BES Support
BigFix Client Compliance Configuration
BigFix Insights for Vulnerability Remediation
Fixlets and Tasks (12)
Baselines (0)
Analyses (0)
Computer Groups (0)
Actions (0)
Subscribed Computers (3)
Dashboards
BigFix ServiceNow Data Flow
CIS Checklist for DB2 on Windows
CIS Checklist for MS SQL Server 2017
CIS Checklist for MS SQL Server 2019
DISA STIG Checklist for RHEL 8
Insights
Patches for Windows
Custom Sites (2)
Operator Sites (0)
LDAP Directories (0)
Roles (0)
Fixlets and Tasks
Search Fixlets and Tasks
Task: Deploy BigFix Insights for Vulnerability Remediation
Take Action Edit Copy Export Hide Locally Hide Globally Remove
Description Details Applicable Computers (1) Action History (2)
Activate Windows
Go to Settings to activate Windows.

Name	Source Sev...	Site	Applicable Compu...	Open Action ...	Category	Download Size	Source	Source ID	Source Rele...
Deploy BigFix Insights for Vulnerability Remediation		IVR 1126	1 / 2	2	Deployment		HCL BigFix ...		12/1/2021
Download BigFix Insights for Vulnerability Remediation Reports		IVR 1126	1 / 2	0	Deployment		HCL BigFix ...		12/1/2021
Manage BigFix Insights for Vulnerability Remediation Datasources		IVR 1126	1 / 2	2	Deployment		HCL BigFix ...		12/1/2021
Manage BigFix Insights for Vulnerability Remediation ETLs		IVR 1126	1 / 2	0	Deployment		HCL BigFix ...		12/1/2021
Manage BigFix Insights for Vulnerability Remediation Service		IVR 1126	1 / 2	0	Deployment		HCL BigFix ...		12/1/2021
Uninstall BigFix Insights for Vulnerability Remediation		IVR 1126	1 / 2	1	Deployment		HCL BigFix ...		12/1/2021

Description

Deploy BigFix Insights for Vulnerability Remediation

This Fixlet will deploy BigFix Insights for Vulnerability Remediation v1.4 to a Windows Server, along with any missing pre-requisites.

Please specify the Deployment Options and configurations below to install and configure the service.

For more details on requirements and configuration, please visit: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html.

Deployment Options

Installation Path
Please provide the desired installation path.

☑ Initialize Schema
When checked, this Fixlet will validate the configuration and attempt to initialize the datasource schemas. If unchecked, the database will have to be initialized manually.

☑ Start Services
When checked, this Fixlet will validate the configuration and start the service after it is installed. If unchecked, the BigFix Insights for Vulnerability Remediation Service will have to be started manually.

Configure Insights Datasource

Database Hostname
Please provide the hostname, DNS name, or IP Address for the Insights Database.

Database
Please provide the database name.

Account
Please provide the username for the BigFix Insights database.

   b. Fill in the blanks in the description panel and **Take action** to deploy the IVR services.

      Please provide:

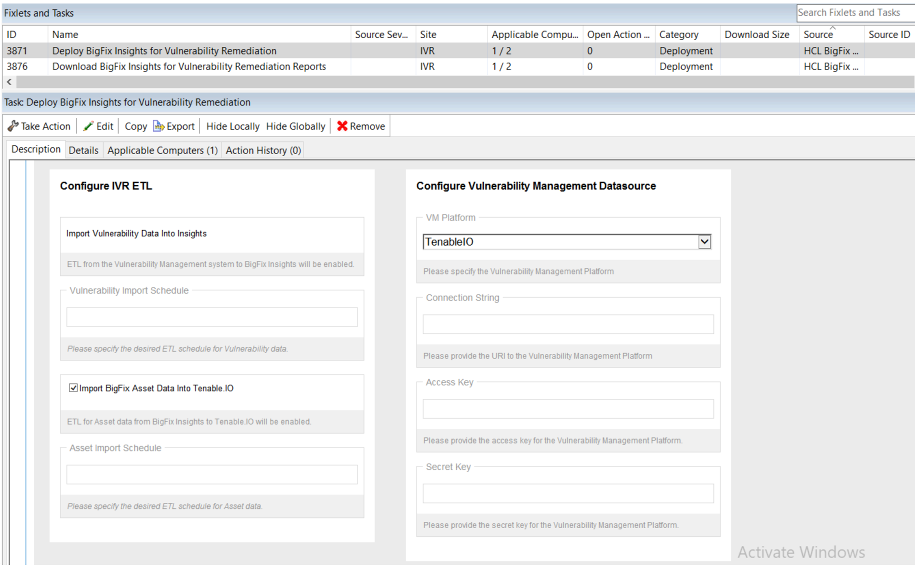
      - Deployment Options
        - Installation path

- Configure Insights Datasource
  - Database Hostname - the hostname, DNS name, or IP address for the Insights Database
  - Database - database name
  - Account - the user name for the BigFix Insights Database
  - Password - the password for the user name specified above
- Configure IVR ETL
  - Import Vulnerability Data Into Insights - specify the desired ETL schedule for Vulnerability data
  - Import BigFix Asset Data Into Tenable.IO - specify the desired ETL schedule for Asset data*

  ETL schedule for Vulnerability data uses Cron Time String Format. Refer to the link to find out more about the Scheduler.

  The column named datasource_device_id in Bigfix Insight serves as the device identifier for IVR purposes. This identifier is labeled as bigfix_asset_id and forwarded to TenableIO.

  *Tenable.IO offers an optional feature that allows BigFix IVR to transmit endpoint asset data to Tenable.IO. This can potentially give Tenable users access to information about assets that were previously unknown. By providing a more comprehensive and current view of the assets, Tenable.IO and BigFix can help in identifying and mitigating potential security risks, identifying under-utilized resources, and facilitating compliance efforts. For more information about assets in Tenable.IO refer to the following page: https://docs.tenable.com/tenableio/Content/Platform/Explore/ExploreAssets.htm.



ID	Name	Source Sev...	Site	Applicable Compu...	Open Action ...	Category	Download Size	Source	Source ID
3871	Deploy BigFix Insights for Vulnerability Remediation		IVR	1 / 2	0	Deployment		HCL BigFix ...	
3876	Download BigFix Insights for Vulnerability Remediation Reports		IVR	1 / 2	0	Deployment		HCL BigFix ...	

Task: Deploy BigFix Insights for Vulnerability Remediation

Configure IVR ETL

Import Vulnerability Data Into Insights

ETL from the Vulnerability Management system to BigFix Insights will be enabled.

Vulnerability Import Schedule

Please specify the desired ETL schedule for Vulnerability data.

☑ Import BigFix Asset Data Into Tenable.IO

ETL for Asset data from BigFix Insights to Tenable.IO will be enabled.

Asset Import Schedule

Please specify the desired ETL schedule for Asset data.

Configure Vulnerability Management Datasource

VM Platform: TenableIO

Please specify the Vulnerability Management Platform

Connection String

Please provide the URI to the Vulnerability Management Platform

Access Key

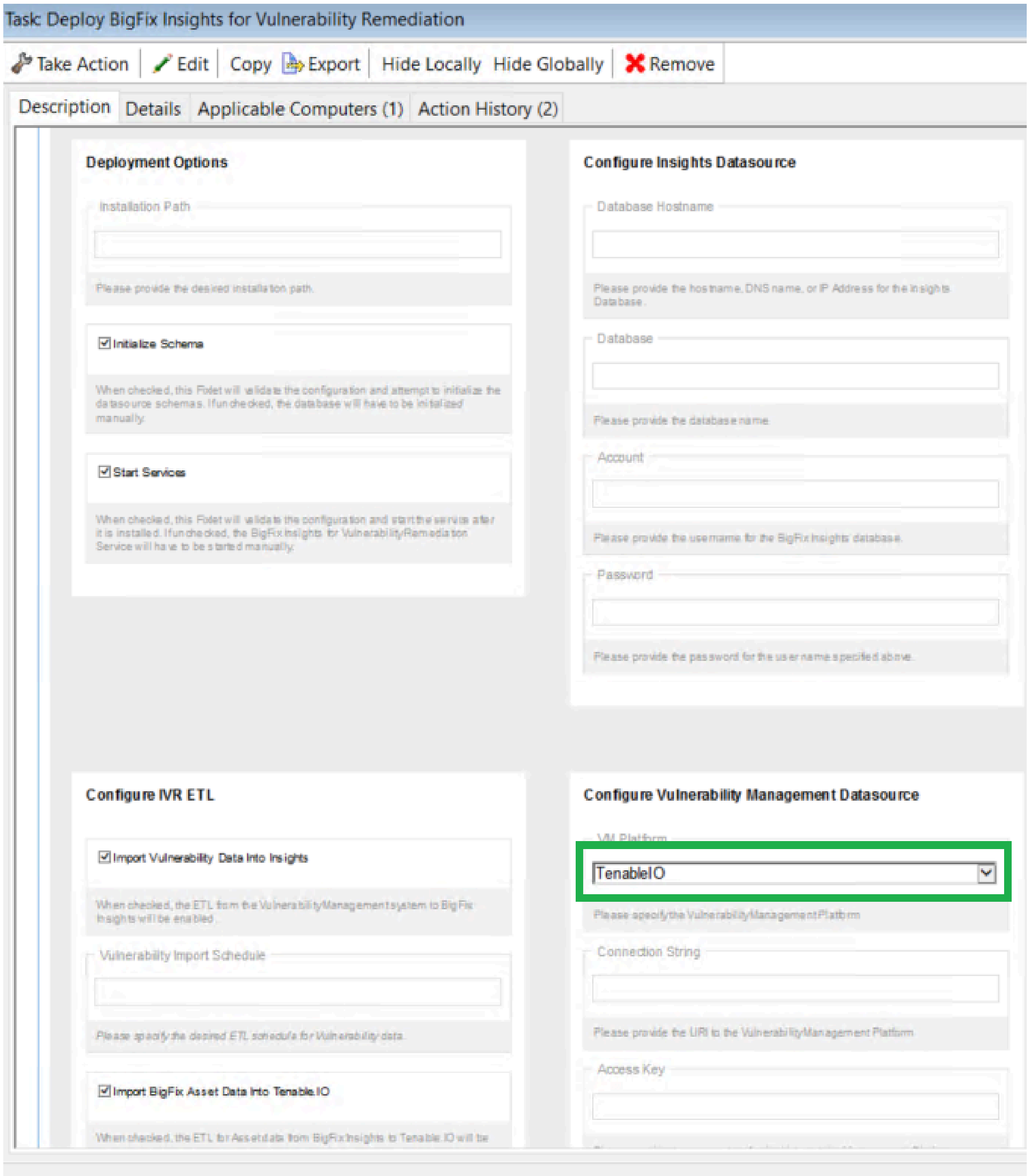
Please provide the access key for the Vulnerability Management Platform.

Secret Key

Please provide the secret key for the Vulnerability Management Platform.

- Configure Vulnerability Management Datasource

- VM Platform - specify the VM Platform
- Connection String - the URL to the Vulnerability Management Platform
- Access Key - access key for the Vulnerability Management Platform
- Secret Key - secret key for the user name specified above



Task: Deploy BigFix Insights for Vulnerability Remediation

Deployment Options

Installation Path

Please provide the desired installation path.

☑ Initialize Schema

When checked, this Fixlet will validate the configuration and attempt to initialize the datasource schemas. If unchecked, the database will have to be initialized manually.

☑ Start Services

When checked, this Fixlet will validate the configuration and start the service after it is installed. If unchecked, the BigFix Insights for VulnerabilityRemediation Service will have to be started manually.

Configure Insights Datasource

Database Hostname

Please provide the hostname, DNS name, or IP Address for the Insights Database.

Database

Please provide the database name.

Account

Please provide the username for the BigFix Insights database.

Password

Please provide the password for the user name specified above.

Configure IVR ETL

☑ Import Vulnerability Data Into Insights

When checked, the ETL from the VulnerabilityManagement system to BigFix Insights will be enabled.

Vulnerability Import Schedule

Please specify the desired ETL schedule for Vulnerability data.

☑ Import BigFix Asset Data Into Tenable.IO

When checked, the ETL for Asset data from BigFix Insights to Tenable.IO will be

Configure Vulnerability Management Datasource

VM Platform

TenableIO

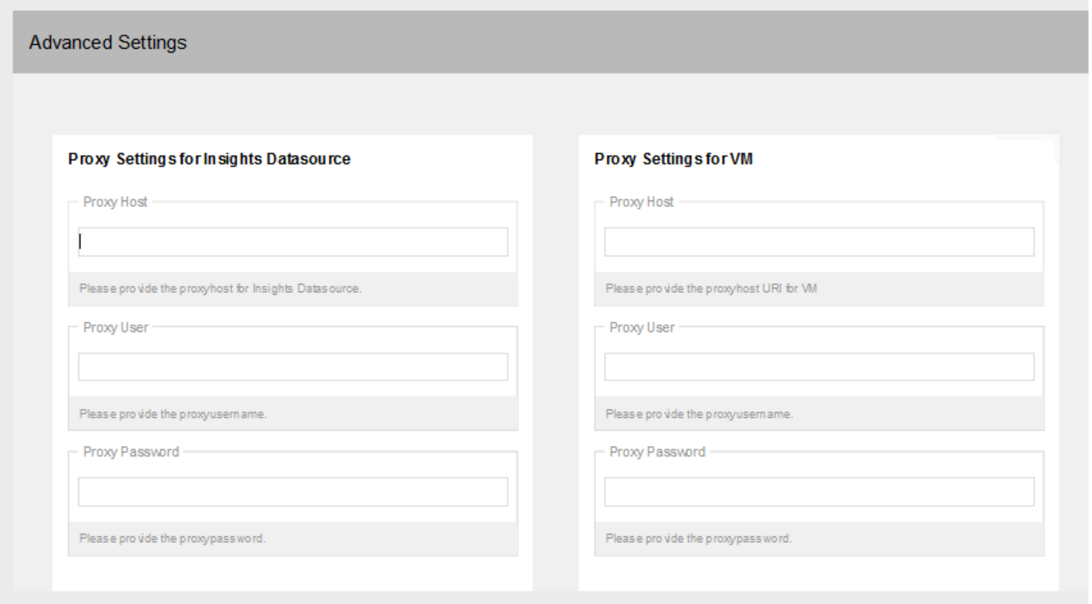
Please specify the VulnerabilityManagementPlatform

Connection String

Please provide the URI to the VulnerabilityManagement Platform

Access Key

To provide proxy details click on **Advanced Settings**. This option is not mandatory.



Advanced Settings

Proxy Settings for Insights Datasource

Proxy Host

Please provide the proxyhost for Insights Datasource.

Proxy User

Please provide the proxyusername.

Proxy Password

Please provide the proxypassword.

Proxy Settings for VM

Proxy Host

Please provide the proxyhost URI for VM

Proxy User

Please provide the proxyusername.

Proxy Password

Please provide the proxypassword.

Note: Please note the following pre-requisites:

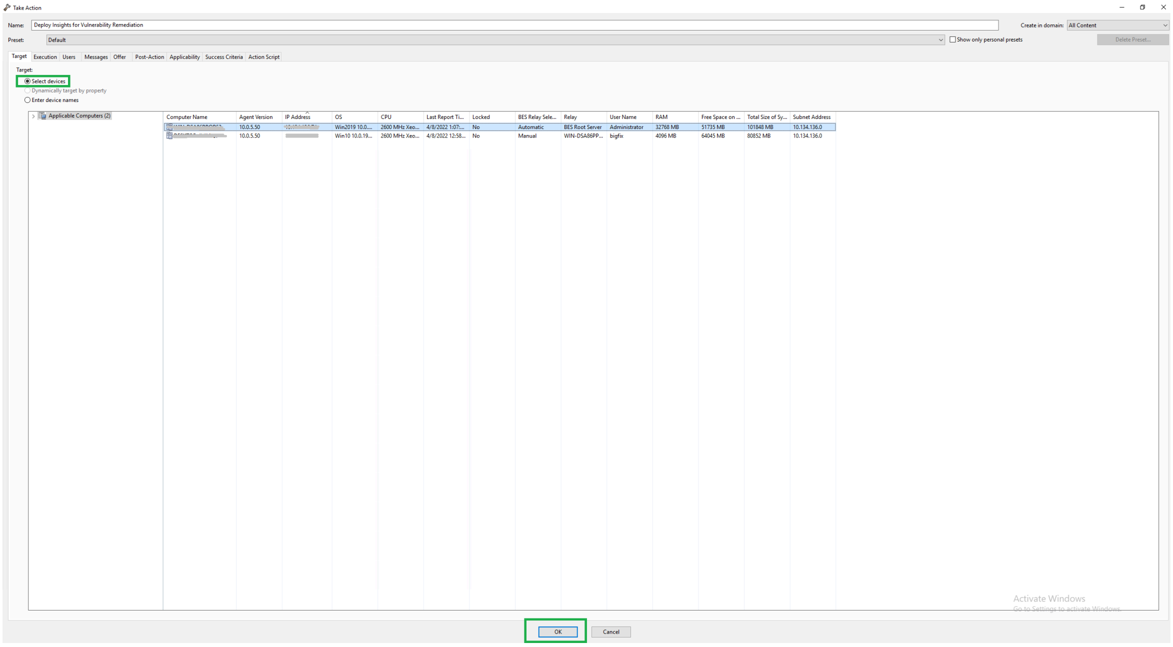
- Microsoft Visual Studio C++ Redistributable 2012:https://www.microsoft.com/en-in/download/details.aspx?id=30679
- Microsoft ODBC Driver 17 for SQL Server: https://www.microsoft.com/en-us/download/details.aspx?id=56567
    - https://www.microsoft.com/en-us/download/details.aspx?id=56567

The Fixlet will attempt to deploy the pre-requisites automatically.

Warning: Do not deploy the **BigFix Insights for Vulnerability Service** to more than 1 machine.

Warning: Do not have more than 2 dataflows per IVR Service.

5. Select target devices under Target tab and click **OK**.



Name: Deploy Insights for Vulnerability Remediation

Create in domain: All Content

Preset: Default

□ Show only personal presets

Target:

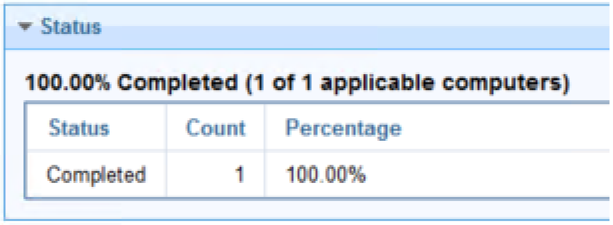
● Select devices

○ Dynamically target by property

○ Enter device names

Computer Name	Agent Version	IP Address	OS	CPU	Last Report Ti...	Locked	BES Relay Sele...	Relay	User Name	RAM	Free Space on ...	Total Size of Sy...	Subnet Address
[redacted]	10.0.5.50	[redacted]	Win2019 10.0....	2600 MHz Xeo...	4/8/2022 1:07:...	No	Automatic	BES Root Server	Administrator	32768 MB	51735 MB	101848 MB	10.134.136.0
[redacted]	10.0.5.50	[redacted]	Win10 10.0.19...	2600 MHz Xeo...	4/8/2022 12:58...	No	Manual	WIN-DSA86PP...	bigfix	4096 MB	64045 MB	80852 MB	10.134.136.0

Wait for the deployment to complete. Status should show 100% completed.



100.00% Completed (1 of 1 applicable computers)

Status	Count	Percentage
Completed	1	100.00%

6. If **Start services** option was selected in the Description panel **BigFix Insights for Vulnerability Remediation** service should be present and in **Running** state in the Services. Otherwise, the **BigFix Insights for Vulnerability Remediation** service must be started manually. This indicates deployment is completed. Deployment can be checked on the log file: install.log.

   Refer to the following link to learn more about other IVR Tasks.

Deployment and configuration for Tenable.sc

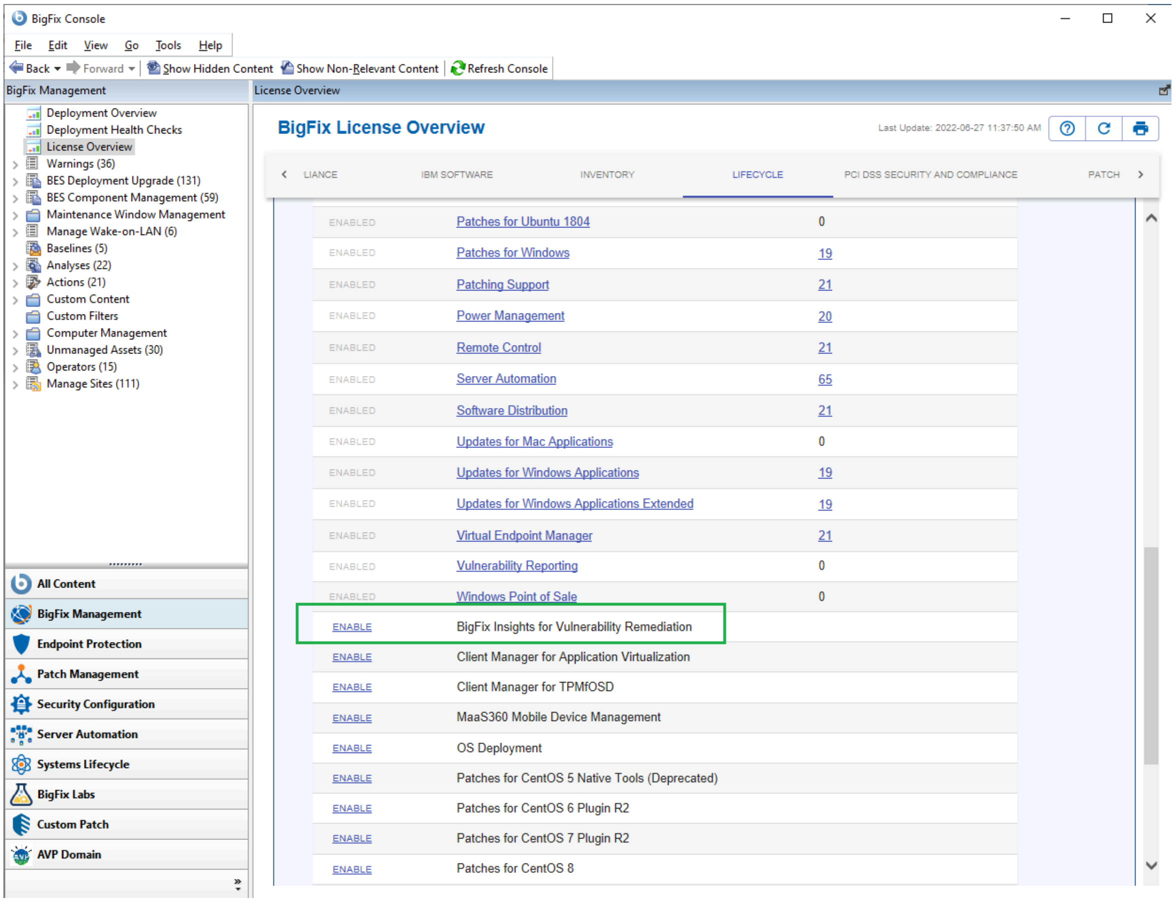
This module provides the steps to deploy and configure the BigFix Insights for Vulnerability Remediation solution.

To install and configure BigFix Insights for Vulnerability Remediation service, perform below steps:

Note: To use the latest release build, the old version must be uninstalled.

1. Enable a content site.

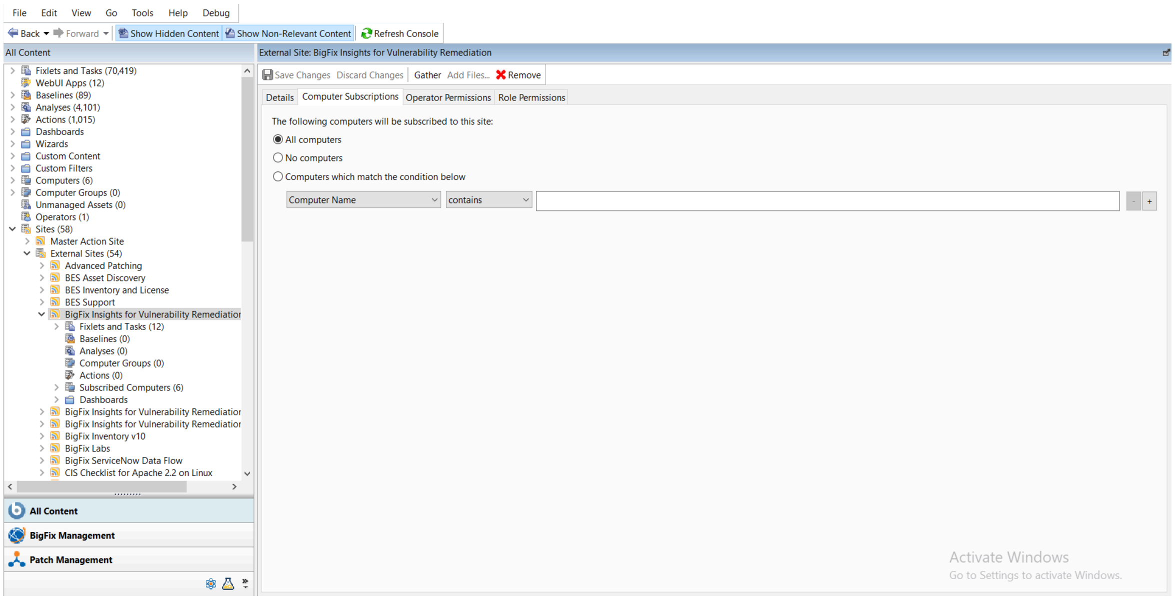
   Navigate to BigFix License Overview Dashboard. In **Compliance/Lifecycle** panel, click **Enable BigFix Insights for Vulnerability Remediation** Fixlet to gather the required content.



ENABLED	Patches for Ubuntu 1804	0
ENABLED	Patches for Windows	19
ENABLED	Patching Support	21
ENABLED	Power Management	20
ENABLED	Remote Control	21
ENABLED	Server Automation	65
ENABLED	Software Distribution	21
ENABLED	Updates for Mac Applications	0
ENABLED	Updates for Windows Applications	19
ENABLED	Updates for Windows Applications Extended	19
ENABLED	Virtual Endpoint Manager	21
ENABLED	Vulnerability Reporting	0
ENABLED	Windows Point of Sale	0
ENABLE	BigFix Insights for Vulnerability Remediation	
ENABLE	Client Manager for Application Virtualization	
ENABLE	Client Manager for TPMfOSD	
ENABLE	MaaS360 Mobile Device Management	
ENABLE	OS Deployment	
ENABLE	Patches for CentOS 5 Native Tools (Deprecated)	
ENABLE	Patches for CentOS 6 Plugin R2	
ENABLE	Patches for CentOS 7 Plugin R2	
ENABLE	Patches for CentOS 8	

   Note: Refer to the following link for more information about **License Overview dashboard**.

2. Subscribe computers to the site. It is recommended to subscribe to All computers. For more information on **Computer Subscriptions Tab** refer to the link.



External Site: BigFix Insights for Vulnerability Remediation

The following computers will be subscribed to this site:

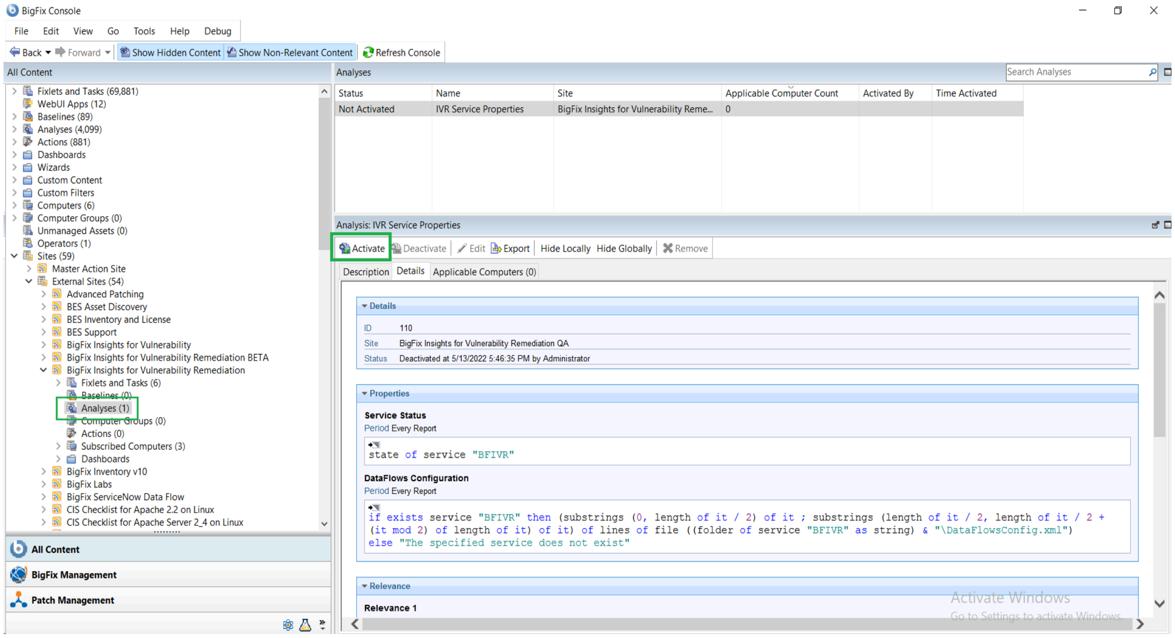
● All computers

○ No computers

○ Computers which match the condition below

Computer Name | contains

3. Activate the analysis.



Status	Name	Site	Applicable Computer Count	Activated By	Time Activated
Not Activated	IVR Service Properties	BigFix Insights for Vulnerability Reme...	0		

Analysis: IVR Service Properties

Details

ID	110
Site	BigFix Insights for Vulnerability Remediation QA
Status	Deactivated at 5/13/2022 5:46:35 PM by Administrator

Properties

Service Status

Period Every Report

```
state of service "BFIVR"
```

DataFlows Configuration

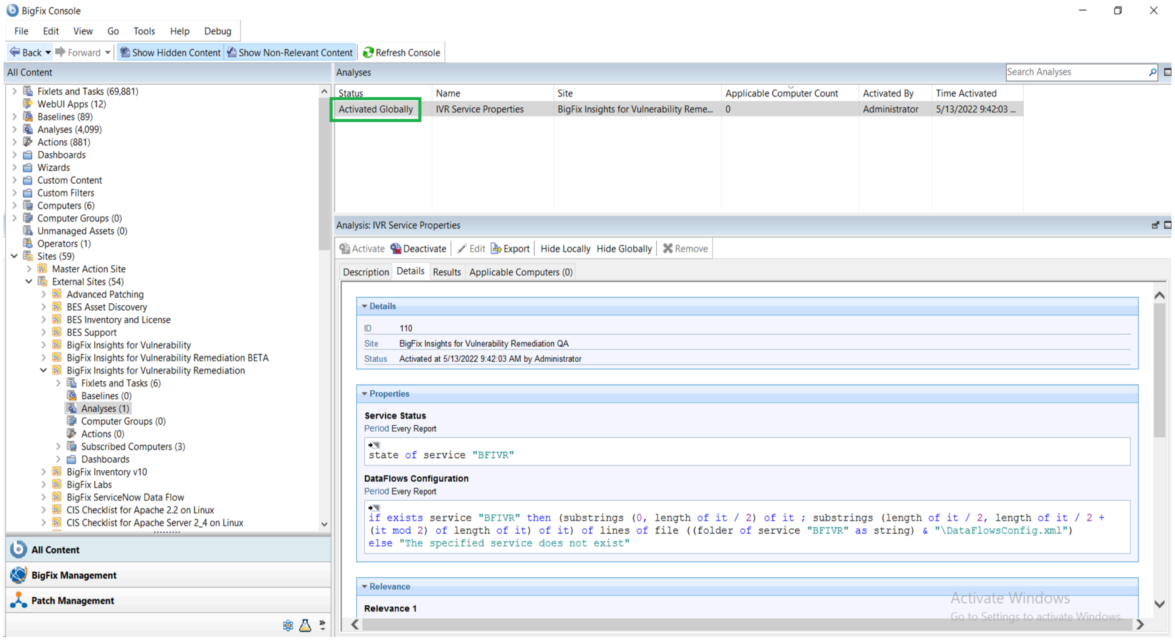
Period Every Report

```
if exists service "BFIVR" then (substrings (0, length of it / 2) of it ; substrings (length of it / 2, length of it / 2 +
(it mod 2) of length of it) of it) of lines of file ((folder of service "BFIVR" as string) & "\DataFlowsConfig.xml")
else "The specified service does not exist"
```

Relevance

Relevance 1

Status of the analysis should be **Activated Globally**.


BigFix Console
File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (69,881)
WebUI Apps (12)
Baselines (89)
Analyses (4,099)
Actions (881)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (6)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (59)
Master Action Site
External Sites (54)
Advanced Patching
BES Asset Discovery
BES Inventory and License
BES Support
BigFix Insights for Vulnerability
BigFix Insights for Vulnerability Remediation BETA
BigFix Insights for Vulnerability Remediation
Fixlets and Tasks (6)
Baselines (0)
Analyses (1)
Computer Groups (0)
Actions (0)
Subscribed Computers (3)
Dashboards
BigFix Inventory v10
BigFix Labs
BigFix ServiceNow Data Flow
CIS Checklist for Apache 2.2 on Linux
CIS Checklist for Apache Server 2_4 on Linux
All Content
BigFix Management
Patch Management
Analyses
Search Analyses
Analysis: IVR Service Properties
Activate Deactivate Edit Export Hide Locally Hide Globally Remove
Description Details Results Applicable Computers (0)
Activate Windows
Go to Settings to activate Windows.

Status	Name	Site	Applicable Computer Count	Activated By	Time Activated
Activated Globally	IVR Service Properties	BigFix Insights for Vulnerability Reme...	0	Administrator	5/13/2022 9:42:03 ...

Details

ID 110
Site BigFix Insights for Vulnerability Remediation QA
Status Activated at 5/13/2022 9:42:03 AM by Administrator

Properties

Service Status
Period Every Report

```
state of service "BFIVR"
```

DataFlows Configuration
Period Every Report

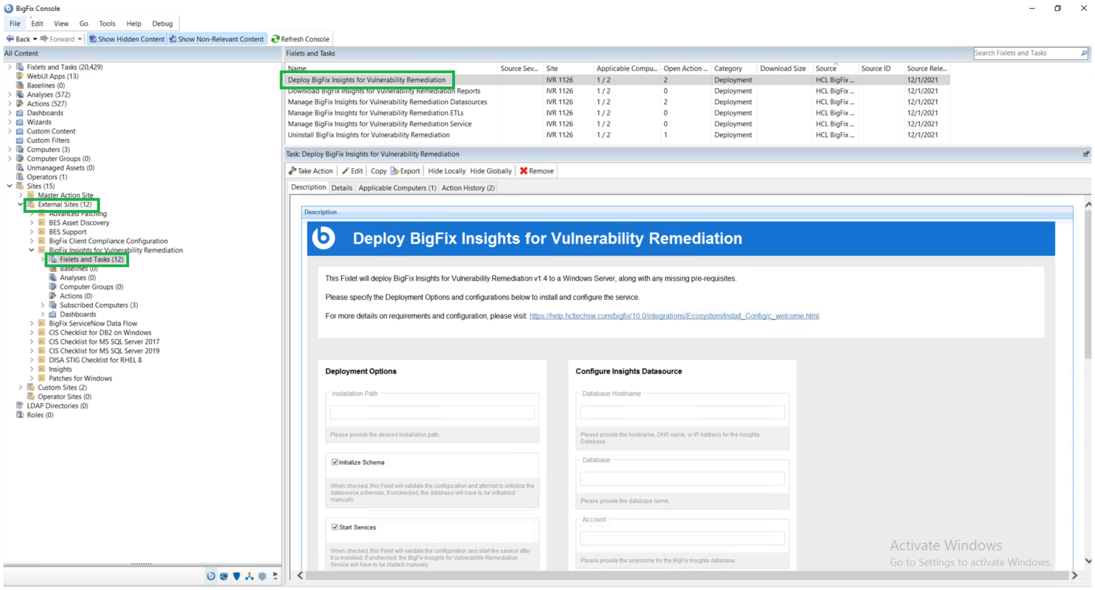
```
if exists service "BFIVR" then (substrings (0, length of it / 2) of it ; substrings (length of it / 2, length of it / 2 +
(it mod 2) of length of it) of it) of lines of file ((folder of service "BFIVR" as string) & "\DataFlowsConfig.xml")
else "The specified service does not exist"
```

Relevance

Relevance 1

Note: Refer to the link to learn more about **Computer Subscriptions** Tab.

4. Deploy the solution to the target server.
    a. Click **Deploy Insights for Vulnerability Remediation** Fixlet in the **BigFix Insights for Vulnerability Remediation** external site.


BigFix Console
File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (20,429)
WebUI Apps (13)
Baselines (0)
Analyses (572)
Actions (527)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (3)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (15)
Master Action Site
External Sites (12)
Advanced Patching
BES Asset Discovery
BES Support
BigFix Client Compliance Configuration
BigFix Insights for Vulnerability Remediation
Fixlets and Tasks (12)
Baselines (0)
Analyses (0)
Computer Groups (0)
Actions (0)
Subscribed Computers (3)
Dashboards
BigFix ServiceNow Data Flow
CIS Checklist for DB2 on Windows
CIS Checklist for MS SQL Server 2017
CIS Checklist for MS SQL Server 2019
DISA STIG Checklist for RHEL 8
Insights
Patches for Windows
Custom Sites (2)
Operator Sites (0)
LDAP Directories (0)
Roles (0)
Fixlets and Tasks
Search Fixlets and Tasks
Task: Deploy BigFix Insights for Vulnerability Remediation
Take Action Edit Copy Export Hide Locally Hide Globally Remove
Description Details Applicable Computers (1) Action History (2)
Activate Windows
Go to Settings to activate Windows.

Name	Source Sev...	Site	Applicable Compu...	Open Action ...	Category	Download Size	Source	Source ID	Source Rele...
Deploy BigFix Insights for Vulnerability Remediation		IVR 1126	1 / 2	2	Deployment		HCL BigFix ...		12/1/2021
Download BigFix Insights for Vulnerability Remediation Reports		IVR 1126	1 / 2	0	Deployment		HCL BigFix ...		12/1/2021
Manage BigFix Insights for Vulnerability Remediation Datasources		IVR 1126	1 / 2	2	Deployment		HCL BigFix ...		12/1/2021
Manage BigFix Insights for Vulnerability Remediation ETLs		IVR 1126	1 / 2	0	Deployment		HCL BigFix ...		12/1/2021
Manage BigFix Insights for Vulnerability Remediation Service		IVR 1126	1 / 2	0	Deployment		HCL BigFix ...		12/1/2021
Uninstall BigFix Insights for Vulnerability Remediation		IVR 1126	1 / 2	1	Deployment		HCL BigFix ...		12/1/2021

Description

Deploy BigFix Insights for Vulnerability Remediation

This Fixlet will deploy BigFix Insights for Vulnerability Remediation v1.4 to a Windows Server, along with any missing pre-requisites.

Please specify the Deployment Options and configurations below to install and configure the service.

For more details on requirements and configuration, please visit: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html.

Deployment Options

Installation Path
Please provide the desired installation path.

☑ Initialize Schema
When checked, this Fixlet will validate the configuration and attempt to initialize the datasource schemas. If unchecked, the database will have to be initialized manually.

☑ Start Services
When checked, this Fixlet will validate the configuration and start the service after it is installed. If unchecked, the BigFix Insights for Vulnerability Remediation Service will have to be started manually.

Configure Insights Datasource

Database Hostname
Please provide the hostname, DNS name, or IP Address for the Insights Database.

Database
Please provide the database name.

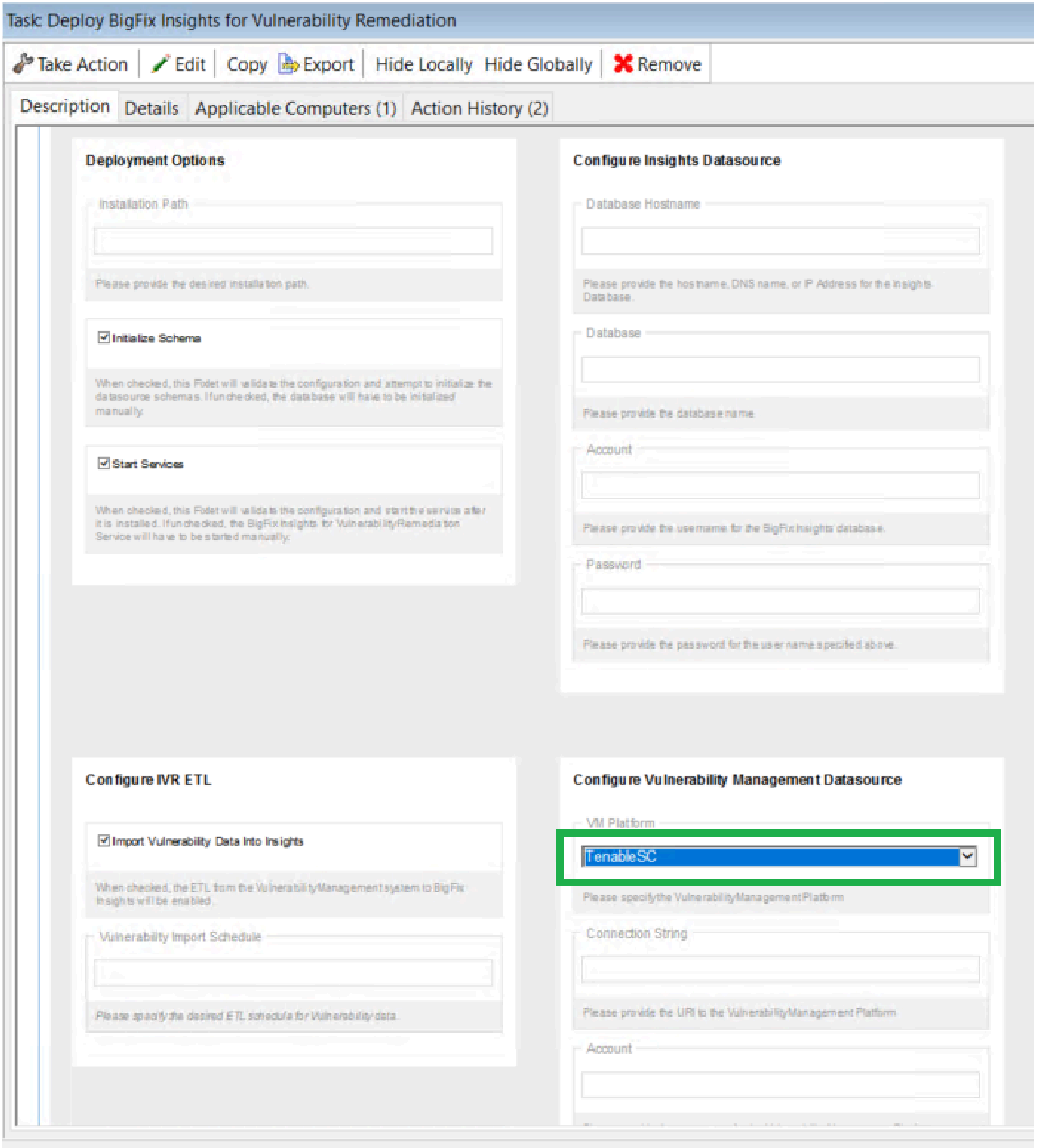
Account
Please provide the username for the BigFix Insights database.

    b. Fill in the blanks in the description panel and **Take action** to deploy the IVR services.

    Please provide:

    - Deployment Options
        - Installation path

- Configure Insights Database
    - Database Hostname - the hostname, DNS name, or IP address for the Insights Database
    - Database - database name
    - Account - the user name for the BigFix Insights Database
    - Password - the password for the user name specified above
- Configure IVR ETL
    - Vulnerability Import Schedule - specify the desired ETL schedule for Vulnerability data. ETL schedule for Vulnerability data uses Cron Time String Format. Refer to the link to find out more about the Scheduler.
- Configure Vulnerability Management Datasource
    - specify the VM Platform
    - Connection String - the URL to the Vulnerability Management Platform
    - Account - the user name for the Vulnerability Management Platform
    - Password - the password for the user name specified above



Deployment Options

Installation Path

Please provide the desired installation path.

☑ Initialize Schema

When checked, this Fixlet will validate the configuration and attempt to initialize the datasource schemas. If unchecked, the database will have to be initialized manually.

☑ Start Services

When checked, this Fixlet will validate the configuration and start the service after it is installed. If unchecked, the BigFix Insights for VulnerabilityRemediation Service will have to be started manually.

Configure Insights Datasource

Database Hostname

Please provide the hostname, DNS name, or IP Address for the Insights Database.

Database

Please provide the database name.

Account

Please provide the username for the BigFix Insights database.

Password

Please provide the password for the user name specified above.

Configure IVR ETL

☑ Import Vulnerability Data Into Insights

When checked, the ETL from the VulnerabilityManagement system to BigFix Insights will be enabled.

Vulnerability Import Schedule

Please specify the desired ETL schedule for Vulnerability data.

Configure Vulnerability Management Datasource

VM Platform

TenableSC

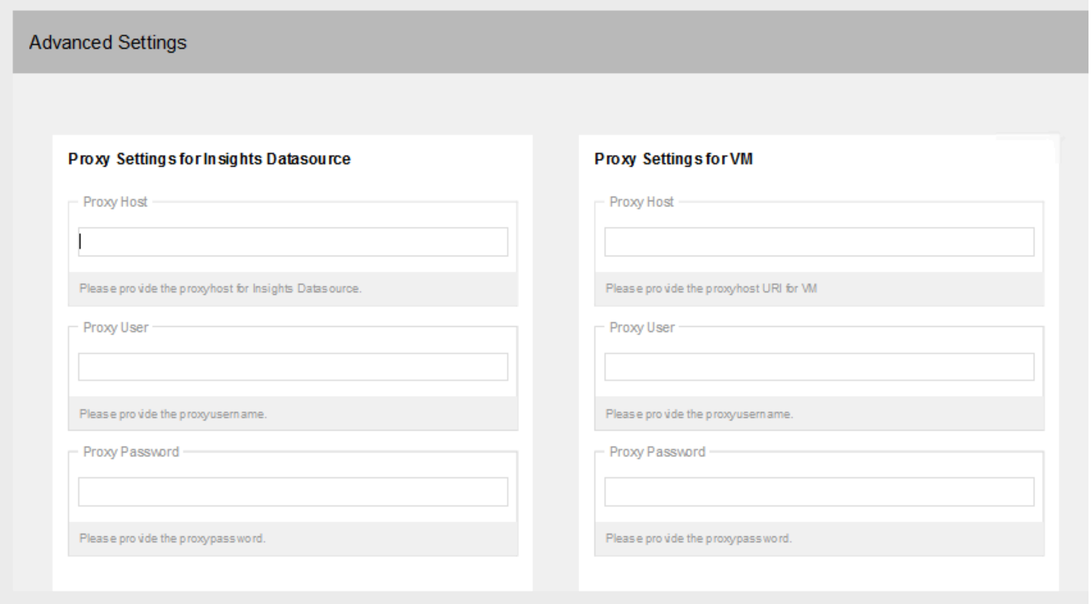
Please specifythe VulnerabilityManagementPlatform

Connection String

Please provide the URI to the VulnerabilityManagement Platform

Account

To provide proxy details click on **Advanced Settings**. This option is not mandatory.



Advanced Settings

Proxy Settings for Insights Datasource

Proxy Host

Please provide the proxyhost for Insights Datasource.

Proxy User

Please provide the proxyusername.

Proxy Password

Please provide the proxypassword.

Proxy Settings for VM

Proxy Host

Please provide the proxyhost URI for VM

Proxy User

Please provide the proxyusername.

Proxy Password

Please provide the proxypassword.

Note: Please note the following pre-requisites:

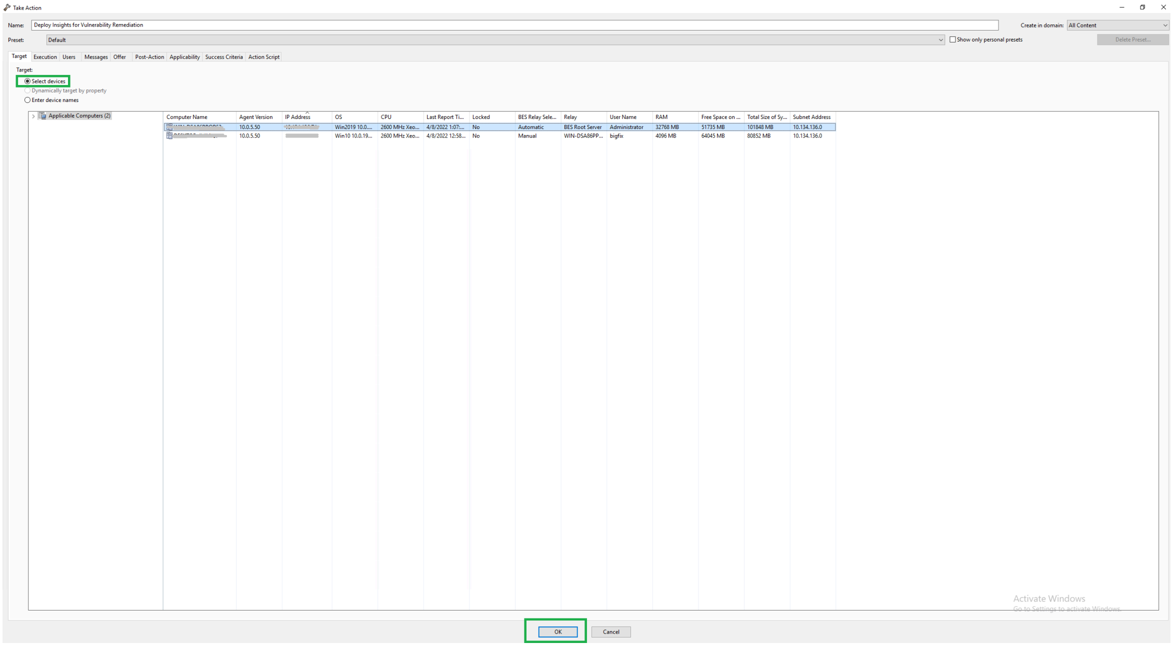
- Microsoft Visual Studio C++ Redistributable 2012:https://www.microsoft.com/en-in/download/details.aspx?id=30679
- Microsoft ODBC Driver 17 for SQL Server: https://www.microsoft.com/en-us/download/details.aspx?id=56567
  - https://www.microsoft.com/en-us/download/details.aspx?id=56567

  The Fixlet will attempt to deploy the pre-requisites automatically.

Warning: Do not deploy the BigFix Insights for Vulnerability Remediation Service to more than 1 machine.

Warning: Do not have more than 1 dataflow per IVR Service.

5. Select target devices and click **OK**.



Take Action

Name: Deploy Insights for Vulnerability Remediation

Create in domain: All Content

Preset: Default

□ Show only personal presets

Target: ● Select devices

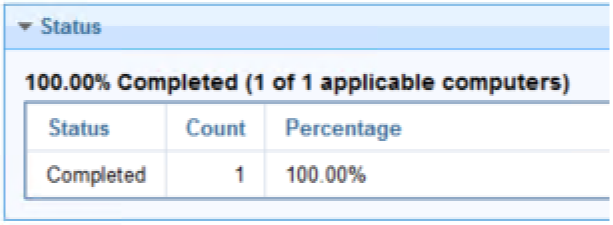
○ Dynamically target by property

○ Enter device names

Applicable Computers (2)

Computer Name	Agent Version	IP Address	OS	CPU	Last Report Ti...	Locked	BES Relay Sele...	Relay	User Name	RAM	Free Space on ...	Total Size of Sy...	Subnet Address
[redacted]	10.0.5.50	[redacted]	Win2019 10.0....	2600 MHz Xeo...	4/8/2022 1:07:...	No	Automatic	BES Root Server	Administrator	32768 MB	51735 MB	101848 MB	10.134.136.0
[redacted]	10.0.5.50	[redacted]	Win10 10.0.19...	2600 MHz Xeo...	4/8/2022 12:58...	No	Manual	WIN-DSA86PP...	bigfix	4096 MB	64045 MB	80852 MB	10.134.136.0

Wait for the deployment to complete. Status should show 100% completed.



Status

100.00% Completed (1 of 1 applicable computers)

Status	Count	Percentage
Completed	1	100.00%

6. If **Start services** option was selected in the Description panel **BigFix Insights for Vulnerability Remediation** service should be present and in **Running** state in the Services. Otherwise, the **BigFix Insights for Vulnerability Remediation** service must be started manually. This indicates deployment is completed. can be checked on the log file: install.log.

   Refer to the following link to learn more about other IVR Tasks.

Deployment and configuration for Qualys

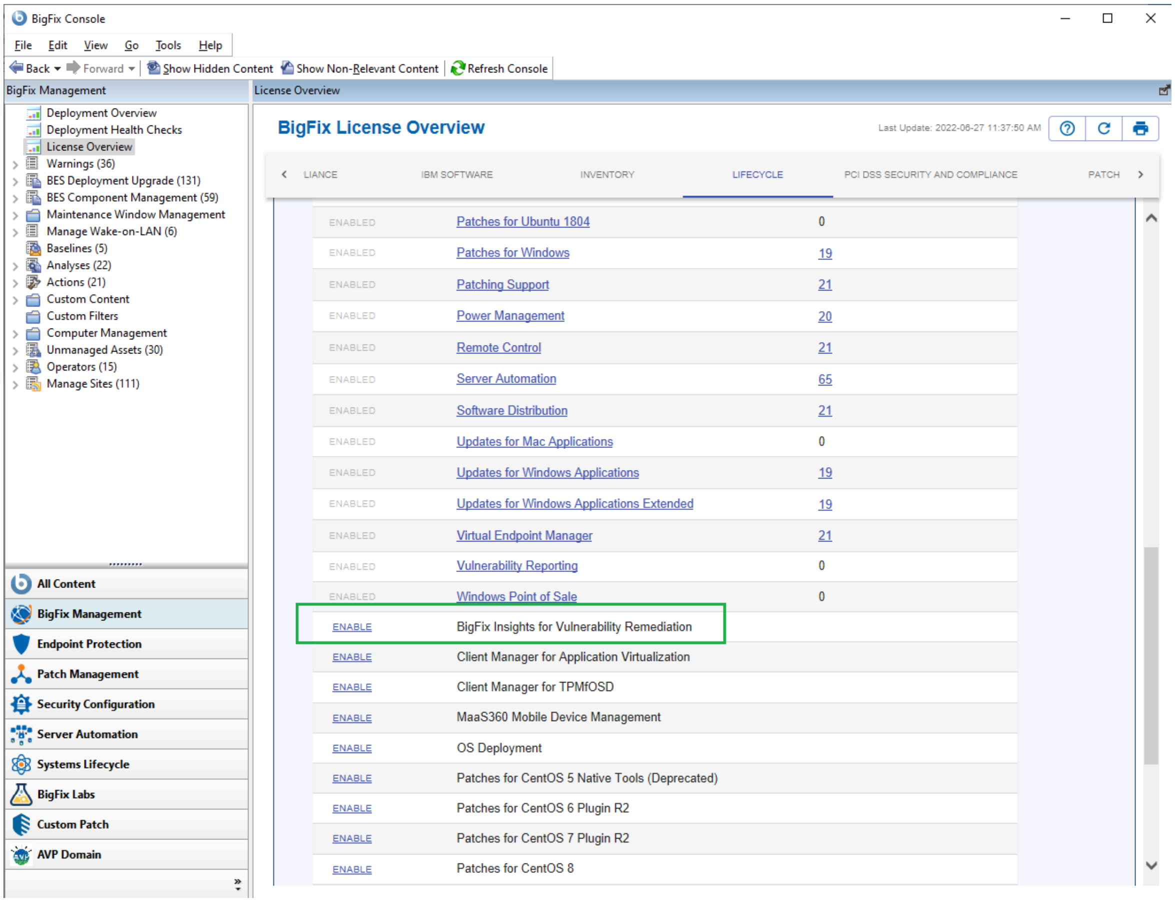
This module provides the steps to deploy and configure the BigFix Insights for Vulnerability Remediation solution.

To install and configure BigFix Insights for Vulnerability Remediation service, perform below steps:

Note: To use the latest release build, the old version must be uninstalled.

1. Enable a content site.

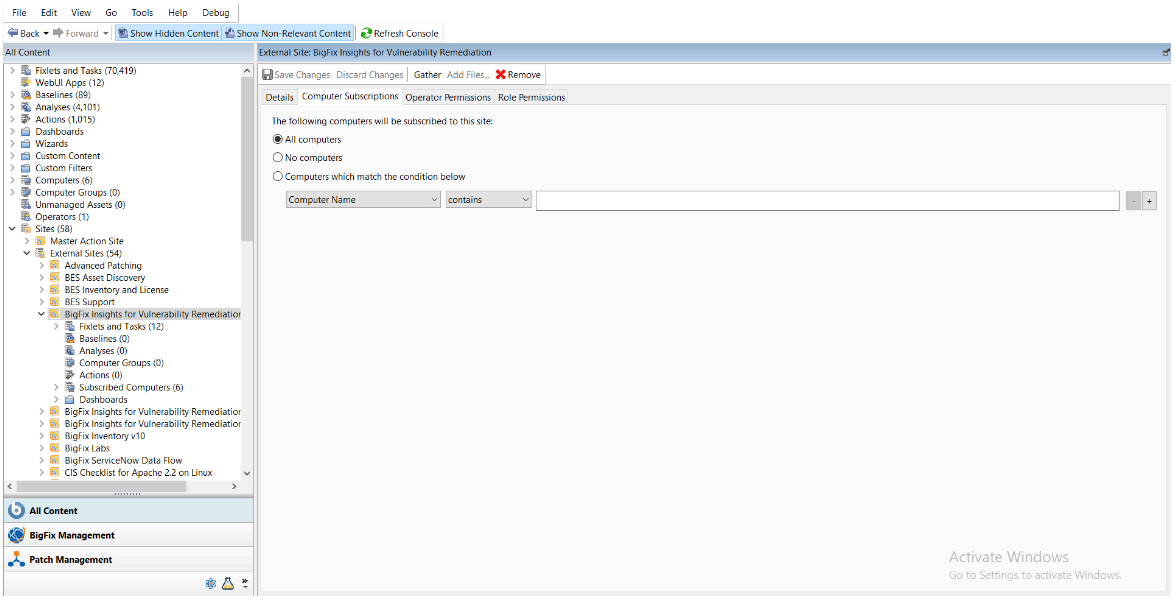
   Navigate to BigFix License Overview Dashboard. In **Compliance/Lifecycle** panel, click **Enable BigFix Insights for Vulnerability Remediation** Fixlet to gather the required content.



ENABLED	Patches for Ubuntu 1804	0
ENABLED	Patches for Windows	19
ENABLED	Patching Support	21
ENABLED	Power Management	20
ENABLED	Remote Control	21
ENABLED	Server Automation	65
ENABLED	Software Distribution	21
ENABLED	Updates for Mac Applications	0
ENABLED	Updates for Windows Applications	19
ENABLED	Updates for Windows Applications Extended	19
ENABLED	Virtual Endpoint Manager	21
ENABLED	Vulnerability Reporting	0
ENABLED	Windows Point of Sale	0
ENABLE	BigFix Insights for Vulnerability Remediation	
ENABLE	Client Manager for Application Virtualization	
ENABLE	Client Manager for TPMfOSD	
ENABLE	MaaS360 Mobile Device Management	
ENABLE	OS Deployment	
ENABLE	Patches for CentOS 5 Native Tools (Deprecated)	
ENABLE	Patches for CentOS 6 Plugin R2	
ENABLE	Patches for CentOS 7 Plugin R2	
ENABLE	Patches for CentOS 8	

   Note: Refer to the following link for more information about **License Overview dashboard**.

2. Subscribe computers to the site. It is recommended to subscribe to All computers. For more information on **Computer Subscriptions Tab** refer to the link.


File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (70,419)
WebUI Apps (12)
Baselines (89)
Analyses (4,101)
Actions (1,015)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (6)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (58)
Master Action Site
External Sites (54)
Advanced Patching
BES Asset Discovery
BES Inventory and License
BES Support
BigFix Insights for Vulnerability Remediatior
Fixlets and Tasks (12)
Baselines (0)
Analyses (0)
Computer Groups (0)
Actions (0)
Subscribed Computers (6)
Dashboards
BigFix Insights for Vulnerability Remediatior
BigFix Insights for Vulnerability Remediatior
BigFix Inventory v10
BigFix Labs
BigFix ServiceNow Data Flow
CIS Checklist for Apache 2.2 on Linux
All Content
BigFix Management
Patch Management
Save Changes Discard Changes Gather Add Files... Remove
Details Computer Subscriptions Operator Permissions Role Permissions
Activate Windows
Go to Settings to activate Windows.

External Site: BigFix Insights for Vulnerability Remediation

The following computers will be subscribed to this site:

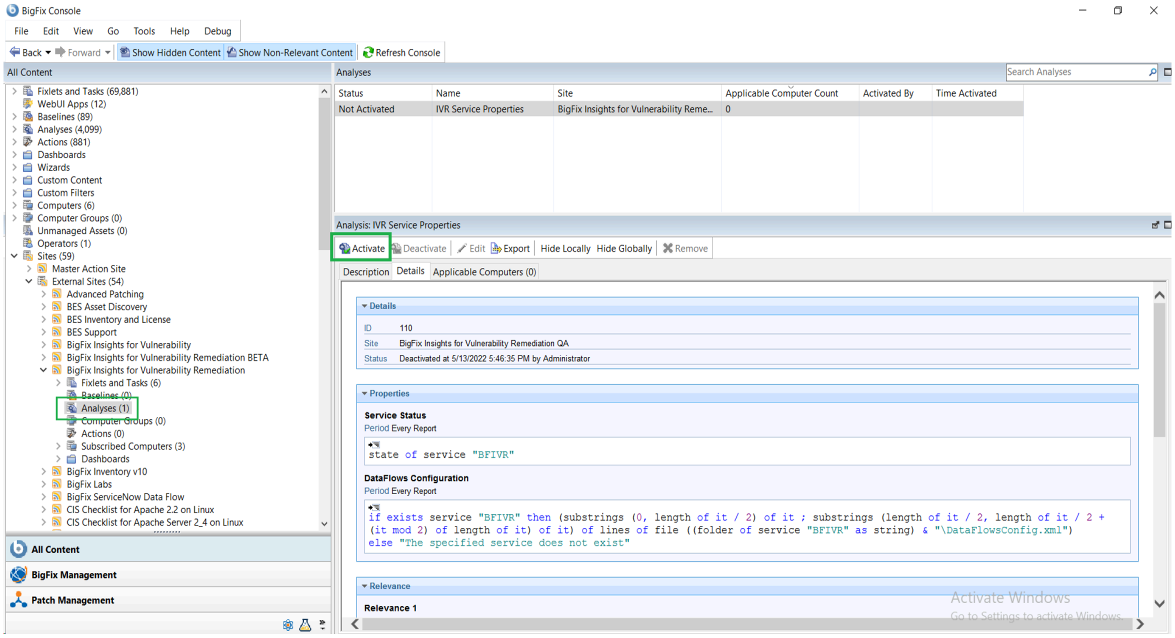
● All computers

○ No computers

○ Computers which match the condition below

Computer Name | contains

3. Activate the analysis.


BigFix Console
File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (69,881)
WebUI Apps (12)
Baselines (89)
Analyses (4,099)
Actions (881)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (6)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (59)
Master Action Site
External Sites (54)
Advanced Patching
BES Asset Discovery
BES Inventory and License
BES Support
BigFix Insights for Vulnerability
BigFix Insights for Vulnerability Remediation BETA
BigFix Insights for Vulnerability Remediation
Fixlets and Tasks (6)
Baselines (0)
Analyses (1)
Computer Groups (0)
Actions (0)
Subscribed Computers (3)
Dashboards
BigFix Inventory v10
BigFix Labs
BigFix ServiceNow Data Flow
CIS Checklist for Apache 2.2 on Linux
CIS Checklist for Apache Server 2_4 on Linux
All Content
BigFix Management
Patch Management
Analyses
Search Analyses
Activate Deactivate Edit Export Hide Locally Hide Globally Remove
Description Details Applicable Computers (0)
Activate Windows
Go to Settings to activate Windows.

Status	Name	Site	Applicable Computer Count	Activated By	Time Activated
Not Activated	IVR Service Properties	BigFix Insights for Vulnerability Reme...	0		

Analysis: IVR Service Properties

Details

ID	110
Site	BigFix Insights for Vulnerability Remediation QA
Status	Deactivated at 5/13/2022 5:46:35 PM by Administrator

Properties

Service Status

Period Every Report

```
state of service "BFIVR"
```

DataFlows Configuration

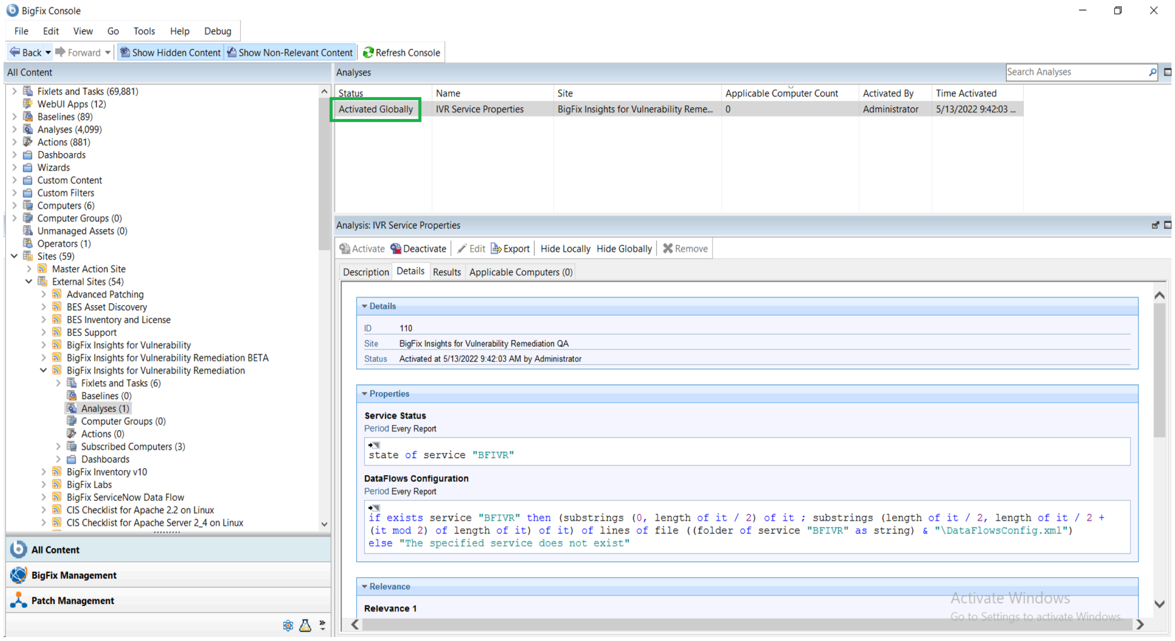
Period Every Report

```
if exists service "BFIVR" then (substrings (0, length of it / 2) of it ; substrings (length of it / 2, length of it / 2 +
(it mod 2) of length of it) of it) of lines of file ((folder of service "BFIVR" as string) & "\DataFlowsConfig.xml")
else "The specified service does not exist"
```

Relevance

Relevance 1

Status of the analysis should be **Activated Globally**.


BigFix Console
File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (69,881)
WebUI Apps (12)
Baselines (89)
Analyses (4,099)
Actions (881)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (6)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (59)
Master Action Site
External Sites (54)
Advanced Patching
BES Asset Discovery
BES Inventory and License
BES Support
BigFix Insights for Vulnerability
BigFix Insights for Vulnerability Remediation BETA
BigFix Insights for Vulnerability Remediation
Fixlets and Tasks (6)
Baselines (0)
Analyses (1)
Computer Groups (0)
Actions (0)
Subscribed Computers (3)
Dashboards
BigFix Inventory v10
BigFix Labs
BigFix ServiceNow Data Flow
CIS Checklist for Apache 2.2 on Linux
CIS Checklist for Apache Server 2_4 on Linux
All Content
BigFix Management
Patch Management
Search Analyses
Activate Deactivate Edit Export Hide Locally Hide Globally Remove
Description Details Results Applicable Computers (0)
Activate Windows
Go to Settings to activate Windows.

Analyses

Status	Name	Site	Applicable Computer Count	Activated By	Time Activated
Activated Globally	IVR Service Properties	BigFix Insights for Vulnerability Reme...	0	Administrator	5/13/2022 9:42:03 ...

Analysis: IVR Service Properties

Details

ID	110
Site	BigFix Insights for Vulnerability Remediation QA
Status	Activated at 5/13/2022 9:42:03 AM by Administrator

Properties

Service Status
Period Every Report

```
state of service "BFIVR"
```

DataFlows Configuration
Period Every Report

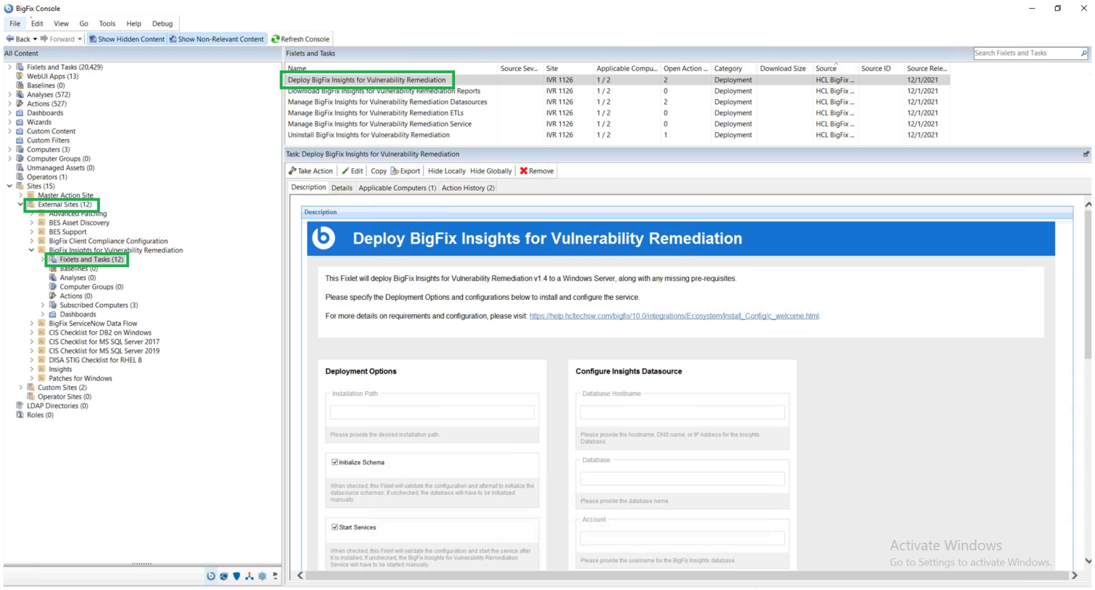
```
if exists service "BFIVR" then (substrings (0, length of it / 2) of it ; substrings (length of it / 2, length of it / 2 +
(it mod 2) of length of it) of it) of lines of file ((folder of service "BFIVR" as string) & "\DataFlowsConfig.xml")
else "The specified service does not exist"
```

Relevance

Relevance 1

Note: Refer to the link to learn more about **Computer Subscriptions** Tab.

4. Deploy the solution to the target server.
   a. Click **Deploy Insights for Vulnerability Remediation** Fixlet in the **BigFix Insights for Vulnerability Remediation** external site.


BigFix Console
File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (20,429)
WebUI Apps (13)
Baselines (0)
Analyses (572)
Actions (527)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (3)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (15)
Master Action Site
External Sites (12)
Advanced Patching
BES Asset Discovery
BES Support
BigFix Client Compliance Configuration
BigFix Insights for Vulnerability Remediation
Fixlets and Tasks (12)
Baselines (0)
Analyses (0)
Computer Groups (0)
Actions (0)
Subscribed Computers (3)
Dashboards
BigFix ServiceNow Data Flow
CIS Checklist for DB2 on Windows
CIS Checklist for MS SQL Server 2017
CIS Checklist for MS SQL Server 2019
DISA STIG Checklist for RHEL 8
Insights
Patches for Windows
Custom Sites (2)
Operator Sites (0)
LDAP Directories (0)
Roles (0)
Search Fixlets and Tasks
Take Action Edit Copy Export Hide Locally Hide Globally Remove
Description Details Applicable Computers (1) Action History (2)
Activate Windows
Go to Settings to activate Windows.

Fixlets and Tasks

Name	Source Sev...	Site	Applicable Compu...	Open Action ...	Category	Download Size	Source	Source ID	Source Rele...
Deploy BigFix Insights for Vulnerability Remediation		IVR 1126	1 / 2	2	Deployment		HCL BigFix ...		12/1/2021
Download BigFix Insights for Vulnerability Remediation Reports		IVR 1126	1 / 2	0	Deployment		HCL BigFix ...		12/1/2021
Manage BigFix Insights for Vulnerability Remediation Datasources		IVR 1126	1 / 2	2	Deployment		HCL BigFix ...		12/1/2021
Manage BigFix Insights for Vulnerability Remediation ETLs		IVR 1126	1 / 2	0	Deployment		HCL BigFix ...		12/1/2021
Manage BigFix Insights for Vulnerability Remediation Service		IVR 1126	1 / 2	0	Deployment		HCL BigFix ...		12/1/2021
Uninstall BigFix Insights for Vulnerability Remediation		IVR 1126	1 / 2	1	Deployment		HCL BigFix ...		12/1/2021

Task: Deploy BigFix Insights for Vulnerability Remediation

Description

Deploy BigFix Insights for Vulnerability Remediation

This Fixlet will deploy BigFix Insights for Vulnerability Remediation v1.4 to a Windows Server, along with any missing pre-requisites.

Please specify the Deployment Options and configurations below to install and configure the service.

For more details on requirements and configuration, please visit: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html.

Deployment Options

Installation Path

Please provide the desired installation path.

☑ Initialize Schema

When checked, this Fixlet will validate the configuration and attempt to initialize the datasource schemas. If unchecked, the database will have to be initialized manually.

☑ Start Services

When checked, this Fixlet will validate the configuration and start the service after it is installed. If unchecked, the BigFix Insights for Vulnerability Remediation Service will have to be started manually.

Configure Insights Datasource

Database Hostname

Please provide the hostname, DNS name, or IP Address for the Insights Database.

Database

Please provide the database name.

Account

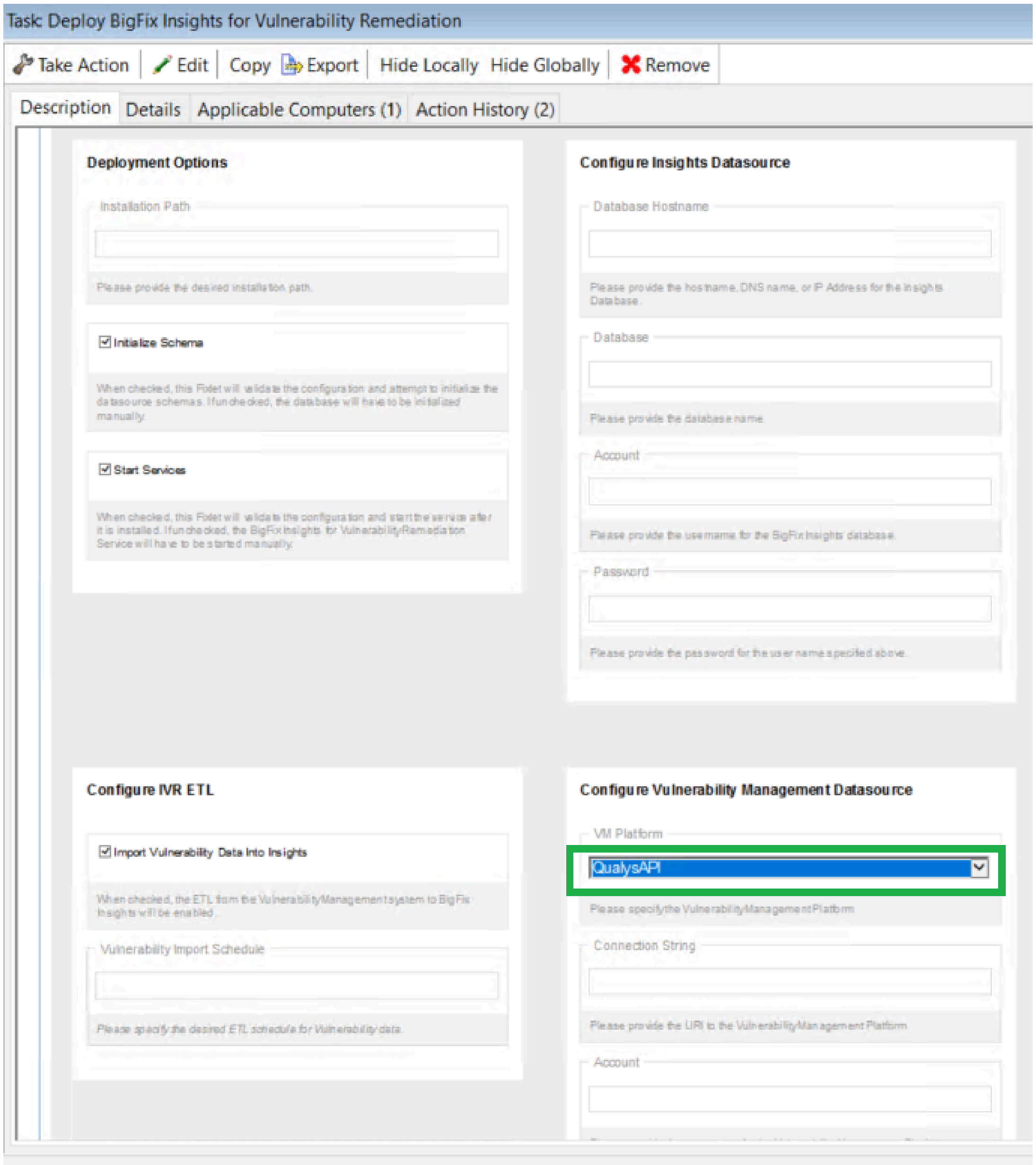
Please provide the username for the BigFix Insights database.

   b. Fill in the blanks in the description panel and **Take action** to deploy the IVR services.

      Please provide:

      - Deployment Options:
        - Installation path

- Configure Insights Database
    - Database Hostname - the hostname, DNS name, or IP address for the Insights Database
    - Database - database name
    - Account - the user name for the BigFix Insights Database
    - Password - the password for the user name specified above
- Configure IVR ETL
    - Vulnerability Import Schedule - ETL schedule for Vulnerability data uses Cron Time String Format. Refer to the link to find out more about the Scheduler
- Configure Vulnerability Management Datasource:
    - specify the VM Platform
    - Connection String - the URL to the Vulnerability Management Platform
    - Account - the user name for the Vulnerability Management Platform
    - Password - the password for the user name specified above



Deployment Options

Installation Path

Please provide the desired installation path.

☑ Initialize Schema

When checked, this Fixlet will validate the configuration and attempt to initialize the datasource schemas. If unchecked, the database will have to be initialized manually.

☑ Start Services

When checked, this Fixlet will validate the configuration and start the service after it is installed. If unchecked, the BigFix Insights for VulnerabilityRemediation Service will have to be started manually.

Configure Insights Datasource

Database Hostname

Please provide the hostname, DNS name, or IP Address for the Insights Database.

Database

Please provide the database name.

Account

Please provide the username for the BigFix Insights database.

Password

Please provide the password for the user name specified above.

Configure IVR ETL

☑ Import Vulnerability Data Into Insights

When checked, the ETL from the VulnerabilityManagement system to BigFix Insights will be enabled.

Vulnerability Import Schedule

Please specify the desired ETL schedule for Vulnerability data.

Configure Vulnerability Management Datasource

VM Platform

QualysAPI

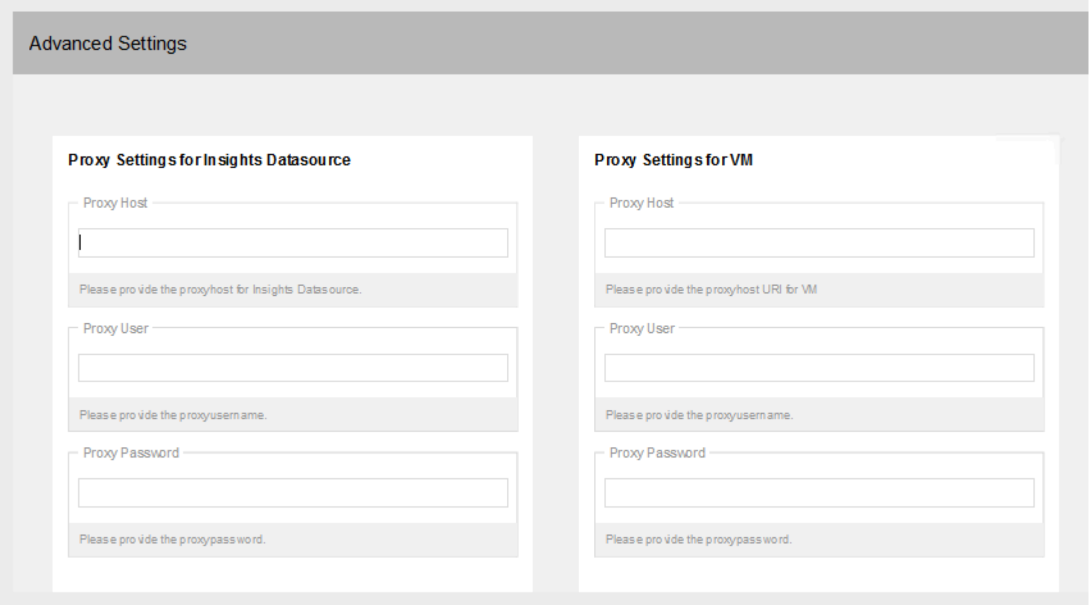
Please specify the VulnerabilityManagementPlatform

Connection String

Please provide the URI to the VulnerabilityManagement Platform

Account

To provide proxy details click on **Advanced Settings**. This option is not mandatory.



Please provide the proxyhost for Insights Datasource.

Please provide the proxyusername.

Please provide the proxypassword.

Please provide the proxyhost URI for VM

Please provide the proxyusername.

Please provide the proxypassword.

Note: Please note the following pre-requisites:

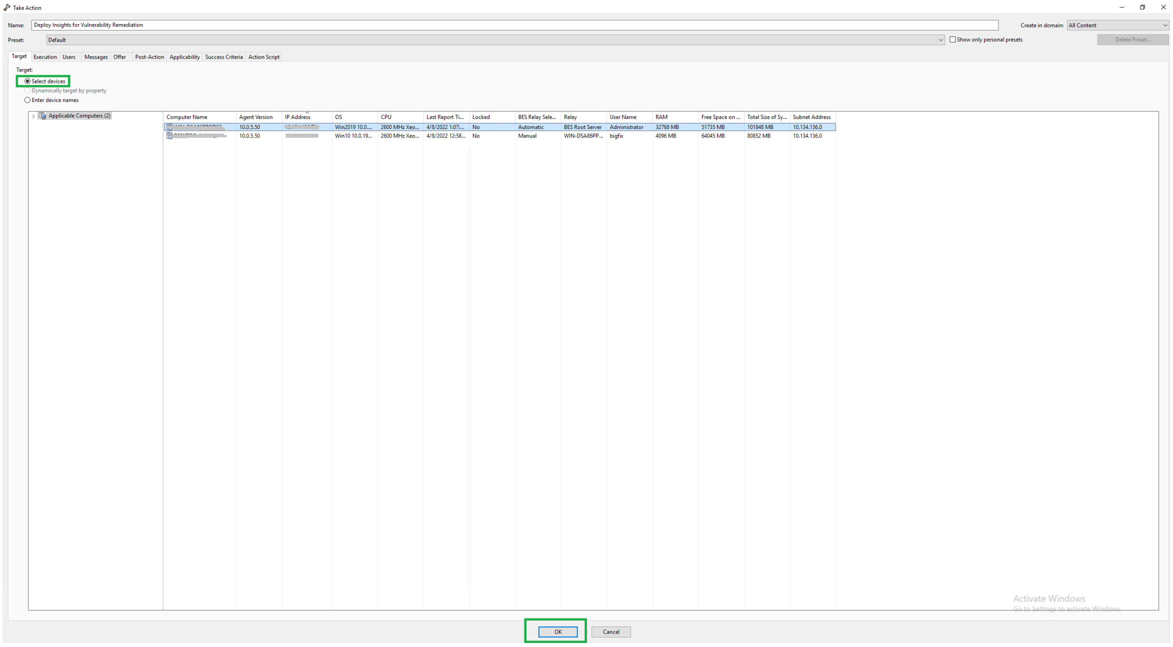
- Microsoft Visual Studio C++ Redistributable 2012:https://www.microsoft.com/en-in/download/details.aspx?id=30679
- Microsoft ODBC Driver 17 for SQL Server: https://www.microsoft.com/en-us/download/details.aspx?id=56567
  - https://www.microsoft.com/en-us/download/details.aspx?id=56567

  The Fixlet will attempt to deploy the pre-requisites automatically.

Warning: Do not deploy the BigFix Insights for Vulnerability Remediation Service to more than 1 machine.

Warning: Do not have more than 1 dataflow per IVR Service.

5. Select target devices and click **OK**. Wait for the deployment to complete.



Take Action

Name: Deploy Insights for Vulnerability Remediation

Create in domain: All Content

Preset: Default

□ Show only personal presets

Target:

● Select devices

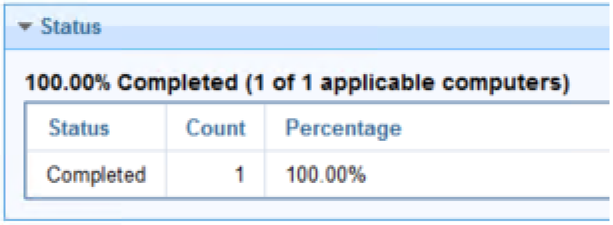
○ Dynamically target by property

○ Enter device names

Applicable Computers (2)

Computer Name	Agent Version	IP Address	OS	CPU	Last Report Ti...	Locked	BES Relay Sele...	Relay	User Name	RAM	Free Space on ...	Total Size of Sy...	Subnet Address
[redacted]	10.0.5.50	[redacted]	Win2019 10.0....	2600 MHz Xeo...	4/8/2022 1:07:...	No	Automatic	BES Root Server	Administrator	32768 MB	51735 MB	101848 MB	10.134.136.0
[redacted]	10.0.5.50	[redacted]	Win10 10.0.19...	2600 MHz Xeo...	4/8/2022 12:58...	No	Manual	WIN-DSA86PP...	bigfix	4096 MB	64045 MB	80852 MB	10.134.136.0

Status should show 100% completed.



Status

100.00% Completed (1 of 1 applicable computers)

Status	Count	Percentage
Completed	1	100.00%

6. If **Start services** option was selected in the Description panel **BigFix Insights for Vulnerability Remediation** service should be present and in **Running** state in the Services. Otherwise, the **BigFix Insights for Vulnerability Remediation** service must be started manually. This indicates deployment is completed. can be checked on the log file: install.log.

   Refer to the following link to learn more about other IVR Tasks.

Chapter 4. Setting up IVR App

Use this module to install and set up your WebUI IVR app.

In order to make WebUI IVR app fully functional, ensure that all the following actions are performed:

1. Deploy **WebUI**.

   Refer to the BigFix WebUI documentation, where you can find information about how to install, maintain, and use *BigFix WebUI*.

2. Deploy **Insights**.

   Refer to the BigFix Insights documentation, where you can find information about how to setup your BigFix Insights.

3. Deploy and configure **IVR Service**.

   Refer to IVR documentation to deploy and configure the BigFix Insights for Vulnerability Remediation solution for the different Vulnerability Management products.

4. Run **ETLs**.

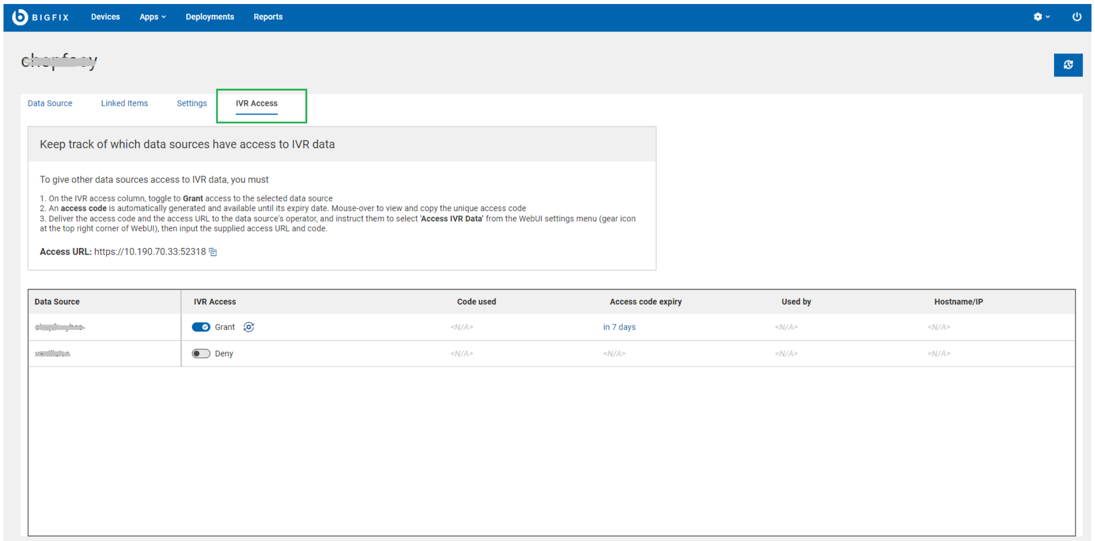
   a. Run Insights ETL - refer to the Insights ETL documentation to learn how to run Insights ETL.
   b. Run IVR dataflow - refer to the IVR dataflow documentation to learn how to run IVR ETL.

5. Configure WebUI IVR Access.

   There are two ways to configure WebUI IVR:

   - As primary datasource

     Once your initial setup of BigFix Insights is performed. Click the **gear icon** in the WebUI navigation bar, select **Insights**, connect to the database and click **Access IVR Data** tab.



Keep track of which data sources have access to IVR data

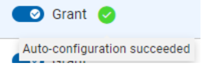
To give other data sources access to IVR data, you must

1. On the IVR access column, toggle to **Grant** access to the selected data source
2. An **access code** is automatically generated and available until its expiry date. Mouse-over to view and copy the unique access code
3. Deliver the access code and the access URL to the data source's operator, and instruct them to select **'Access IVR Data'** from the WebUI settings menu (gear icon at the top right corner of WebUI), then input the supplied access URL and code.

Access URL: https://10.190.70.33:52318

Data Source	IVR Access	Code used	Access code expiry	Used by	Hostname/IP
[redacted]	Grant	<N/A>	in 7 days	<N/A>	<N/A>
[redacted]	Deny	<N/A>	<N/A>	<N/A>	<N/A>

- Toggle to Grant access to the selected data source
- Click ⚙ to automatically configure IVR. Once it is completed symbol will be changed to



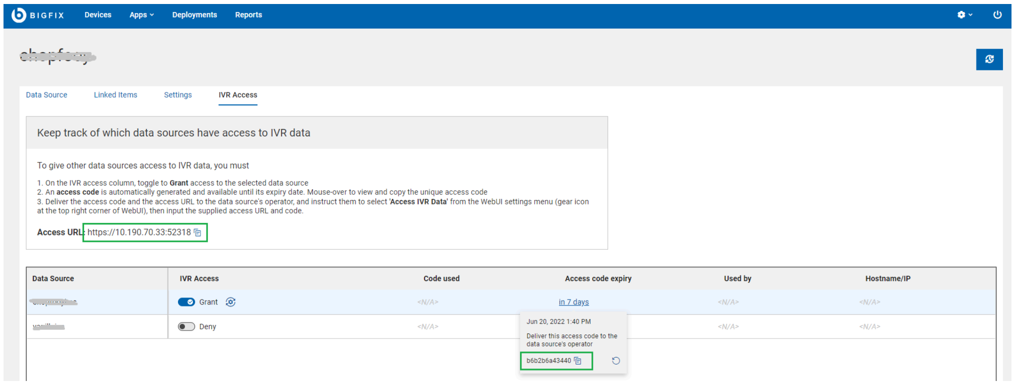
Grant ✓

Auto-configuration succeeded

◦ As secondary datasource

To configure access as a secondary datasource, follow the steps provided in IVR Access tab:

- On the IVR access column, toggle to **Grant** access to the selected data source.
- An **access code** is automatically generated and available until its expiry date. Mouseover to view and copy the unique access code.



[redacted]

Keep track of which data sources have access to IVR data

To give other data sources access to IVR data, you must

1. On the IVR access column, toggle to **Grant** access to the selected data source
2. An **access code** is automatically generated and available until its expiry date. Mouse-over to view and copy the unique access code
3. Deliver the access code and the access URL to the data source's operator, and instruct them to select '**Access IVR Data**' from the WebUI settings menu (gear icon at the top right corner of WebUI), then input the supplied access URL and code.

Access URL: https://10.190.70.33:52318

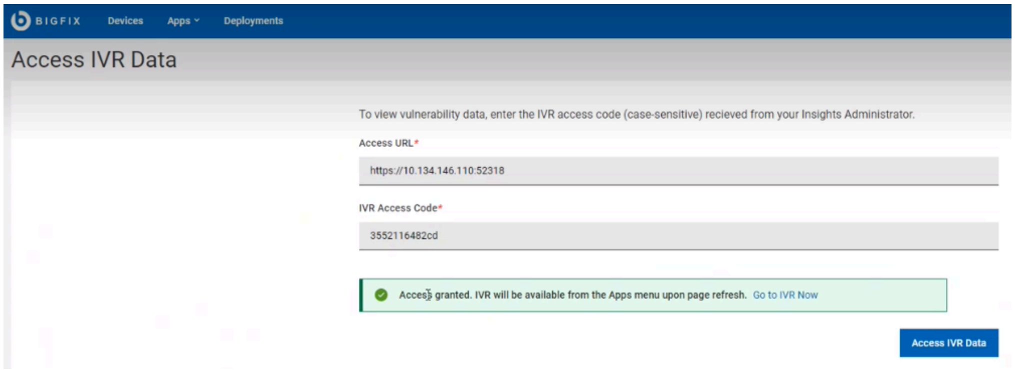
Data Source	IVR Access	Code used	Access code expiry	Used by	Hostname/IP
[redacted]	Grant	<N/A>	in 7 days	<N/A>	<N/A>
[redacted]	Deny	<N/A>		<N/A>	<N/A>

Jun 20, 2022 1:40 PM

Deliver this access code to the data source's operator

b6b2b6a43440

- Deliver the access code and the access URL to the data source's operator and instruct them to select '**Access IVR Data**' from the WebUI settings menu (gear icon at the top right corner of WebUI), then input the supplied access URL and code.



Access IVR Data

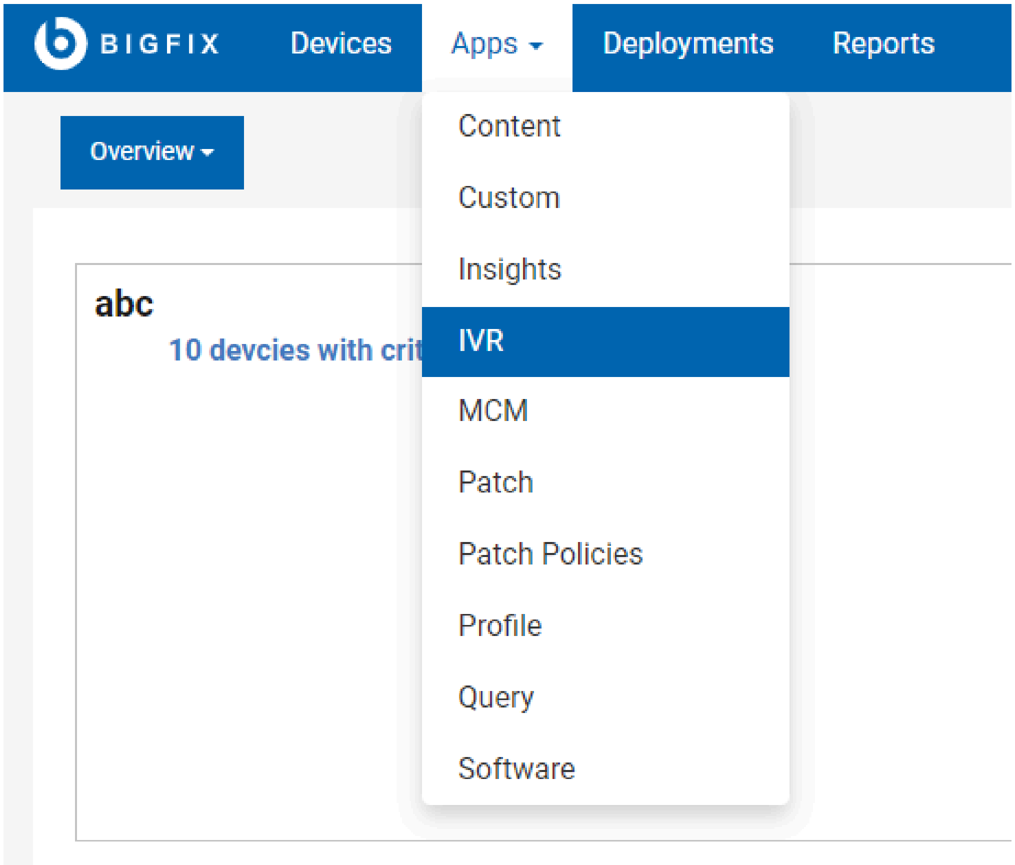
To view vulnerability data, enter the IVR access code (case-sensitive) recieved from your Insights Administrator.

Access URL*: https://10.134.146.110:52318

IVR Access Code*: 3552116482cd

Access granted. IVR will be available from the Apps menu upon page refresh. Go to IVR Now

- Once the access is granted, IVR app appears in the WebUI Apps drop-down menu.



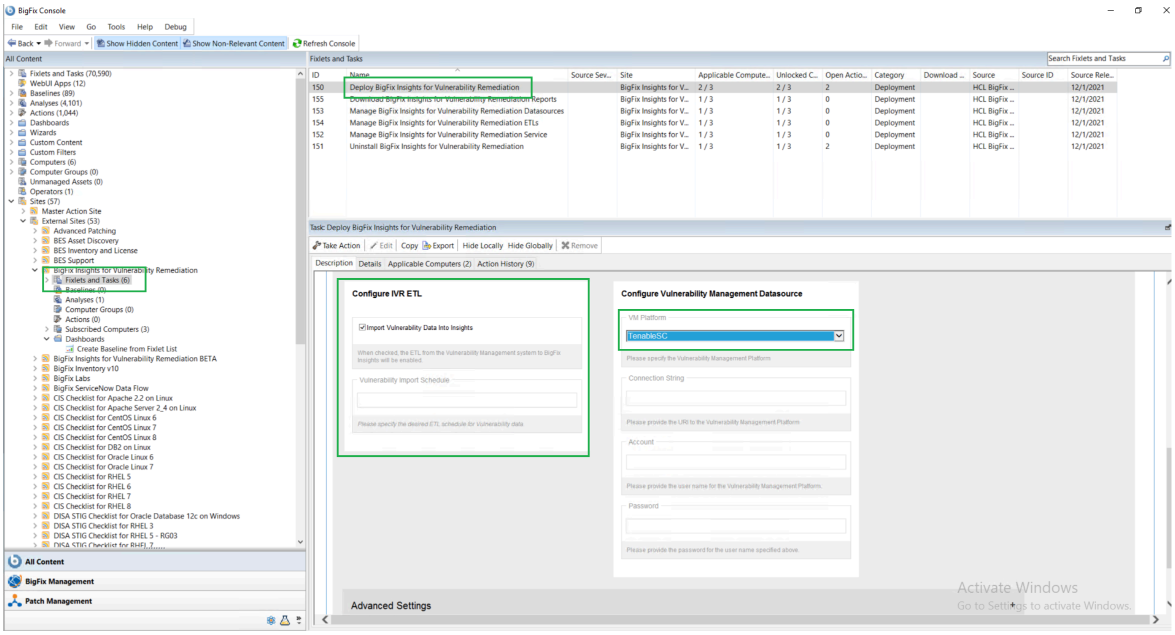
6. IVR App User's Guide

Chapter 5. Scheduling IVR ETL

The Extract, Transform, Load (ETL) process pulls data from a datasource and stores it in the IVR database. An ETL process consumes significant time and resources and hence must be performed on a customized schedule to minimize disruption. In IVR, you can schedule an ETL daily, weekly, or monthly.

Perform the following steps to schedule an ETL in IVR:

1. Initial IVR ETL scheduling is made during deployment. Refer to the link to see how to deploy IVR Service and configure ETL.

ID	Name	Source Sev...	Site	Applicable Compute...	Unlocked C...	Open Actio...	Category	Download ...	Source	Source ID	Source Rele...
150	Deploy BigFix Insights for Vulnerability Remediation		BigFix Insights for V...	2 / 3	2 / 3	2	Deployment		HCL BigFix ...		12/1/2021
155	Download BigFix Insights for Vulnerability Remediation Reports		BigFix Insights for V...	1 / 3	1 / 3	0	Deployment		HCL BigFix ...		12/1/2021
153	Manage BigFix Insights for Vulnerability Remediation Datasources		BigFix Insights for V...	1 / 3	1 / 3	0	Deployment		HCL BigFix ...		12/1/2021
154	Manage BigFix Insights for Vulnerability Remediation ETLs		BigFix Insights for V...	1 / 3	1 / 3	0	Deployment		HCL BigFix ...		12/1/2021
152	Manage BigFix Insights for Vulnerability Remediation Service		BigFix Insights for V...	1 / 3	1 / 3	0	Deployment		HCL BigFix ...		12/1/2021
151	Uninstall BigFix Insights for Vulnerability Remediation		BigFix Insights for V...	1 / 3	1 / 3	2	Deployment		HCL BigFix ...		12/1/2021

   Task: Deploy BigFix Insights for Vulnerability Remediation

   Configure IVR ETL

   ☑ Import Vulnerability Data Into Insights

   When checked, the ETL from the Vulnerability Management system to BigFix Insights will be enabled.

   Vulnerability Import Schedule

   Please specify the desired ETL schedule for Vulnerability data.

   Configure Vulnerability Management Datasource

   VM Platform: TenableSC

   Please specify the Vulnerability Management Platform

   Connection String

   Please provide the URI to the Vulnerability Management Platform

   Account

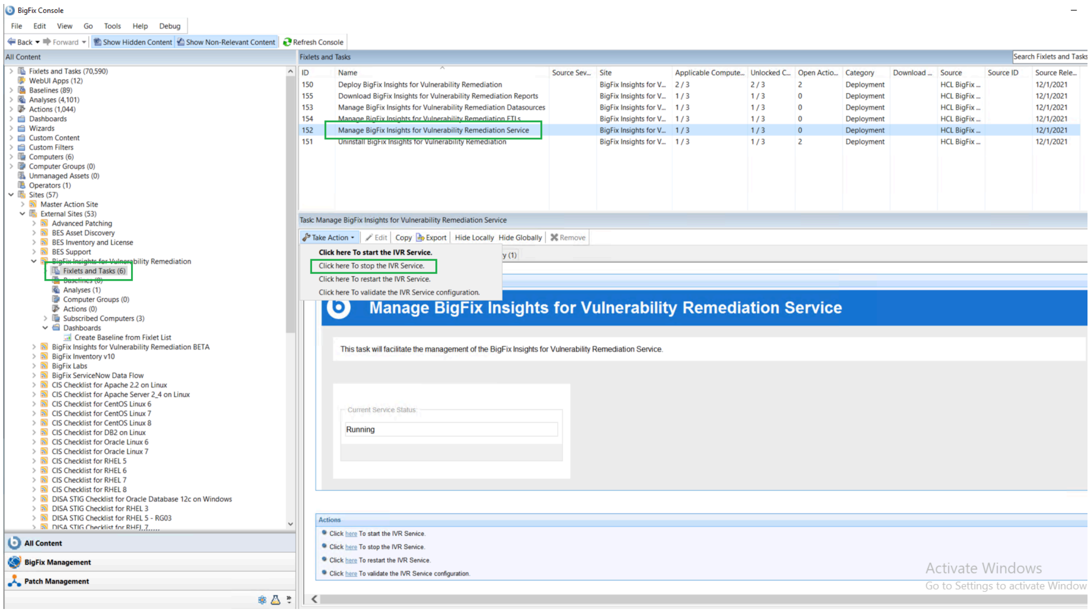
   Please provide the user name for the Vulnerability Management Platform.

   Password

   Please provide the password for the user name specified above.

2. After you complete the initial configuration of IVR Service, you can configure IVR ETL using Manage BigFix Insights for Vulnerability Remediation ETLs Fixlet.

Note: IVR Service must be stopped to perform this task. To stop the service use Manage BigFix Insights for Vulnerability Remediation Service Fixlet and Take Action on Stop IVR Service.


BigFix Console
File Edit View Go Tools Help Debug
Back Forward Show Hidden Content Show Non-Relevant Content Refresh Console
All Content
Fixlets and Tasks (70,590)
WebUI Apps (12)
Baselines (89)
Analyses (4,101)
Actions (1,044)
Dashboards
Wizards
Custom Content
Custom Filters
Computers (6)
Computer Groups (0)
Unmanaged Assets (0)
Operators (1)
Sites (57)
Master Action Site
External Sites (53)
Advanced Patching
BES Asset Discovery
BES Inventory and License
BES Support
BigFix Insights for Vulnerability Remediation
Fixlets and Tasks (6)
Baselines (0)
Analyses (1)
Computer Groups (0)
Actions (0)
Subscribed Computers (3)
Dashboards
Create Baseline from Fixlet List
BigFix Insights for Vulnerability Remediation BETA
BigFix Inventory v10
BigFix Labs
BigFix ServiceNow Data Flow
CIS Checklist for Apache 2.2 on Linux
CIS Checklist for Apache Server 2_4 on Linux
CIS Checklist for CentOS Linux 6
CIS Checklist for CentOS Linux 7
CIS Checklist for CentOS Linux 8
CIS Checklist for DB2 on Linux
CIS Checklist for Oracle Linux 6
CIS Checklist for Oracle Linux 7
CIS Checklist for RHEL 5
CIS Checklist for RHEL 6
CIS Checklist for RHEL 7
CIS Checklist for RHEL 8
DISA STIG Checklist for Oracle Database 12c on Windows
DISA STIG Checklist for RHEL 3
DISA STIG Checklist for RHEL 5 - RG03
DISA STIG Checklist for RHEL 7
All Content
BigFix Management
Patch Management
Fixlets and Tasks
Search Fixlets and Tasks
Take Action Edit Copy Export Hide Locally Hide Globally Remove
Activate Windows
Go to Settings to activate Windows

ID	Name	Source Sev...	Site	Applicable Compute...	Unlocked C...	Open Actio...	Category	Download ...	Source	Source ID	Source Rele...
150	Deploy BigFix Insights for Vulnerability Remediation		BigFix Insights for V...	2 / 3	2 / 3	2	Deployment		HCL BigFix ...		12/1/2021
155	Download BigFix Insights for Vulnerability Remediation Reports		BigFix Insights for V...	1 / 3	1 / 3	0	Deployment		HCL BigFix ...		12/1/2021
153	Manage BigFix Insights for Vulnerability Remediation Datasources		BigFix Insights for V...	1 / 3	1 / 3	0	Deployment		HCL BigFix ...		12/1/2021
154	Manage BigFix Insights for Vulnerability Remediation ETLs		BigFix Insights for V...	1 / 3	1 / 3	0	Deployment		HCL BigFix ...		12/1/2021
152	Manage BigFix Insights for Vulnerability Remediation Service		BigFix Insights for V...	1 / 3	1 / 3	0	Deployment		HCL BigFix ...		12/1/2021
151	Uninstall BigFix Insights for Vulnerability Remediation		BigFix Insights for V...	1 / 3	1 / 3	2	Deployment		HCL BigFix ...		12/1/2021

Task: Manage BigFix Insights for Vulnerability Remediation Service

Click here To start the IVR Service.
Click here To stop the IVR Service.
Click here To restart the IVR Service.
Click here To validate the IVR Service configuration.

Manage BigFix Insights for Vulnerability Remediation Service

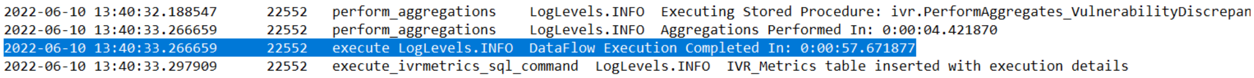
This task will facilitate the management of the BigFix Insights for Vulnerability Remediation Service.

Current Service Status: Running

Actions
- Click here To start the IVR Service.
- Click here To stop the IVR Service.
- Click here To restart the IVR Service.
- Click here To validate the IVR Service configuration.

To ensure that dataflow has completed successfully, go to logs folder and open a respective dataflow_*.log file. Check if the following message appears in the file:

```
execute LogLevels.INFO DataFlow Execution Completed
```



```
2022-06-10 13:40:32.188547    22552   perform_aggregations    LogLevels.INFO  Executing Stored Procedure: ivr.PerformAggregates_VulnerabilityDiscrepan
2022-06-10 13:40:33.266659    22552   perform_aggregations    LogLevels.INFO  Aggregations Performed In: 0:00:04.421870
2022-06-10 13:40:33.266659    22552   execute LogLevels.INFO  DataFlow Execution Completed In: 0:00:57.671877
2022-06-10 13:40:33.297909    22552   execute_ivrmetrics_sql_command  LogLevels.INFO  IVR_Metrics table inserted with execution details
```

Chapter 6. IVR Fixlets and Tasks

Learn more about available Fixlets and Tasks for BigFix Insights for Vulnerability Remediation.

Deploy Insights for Vulnerability Remediation

Tenable.io

Tenable.sc

Qualys

Download BigFix Insights for Vulnerability Remediation Reports

Use this task to deploy the reports for PowerBI or Tableau platform.

BigFix Insights for Vulnerability Remediation provides business intelligence reports to address three main use cases:

- **Vulnerabilities With Available Fixlets** - A list of vulnerabilities that have matching BigFix Fixlets available for remediation. The report will list the most recent Fixlet related to each vulnerability, and the CVE entries that are associated to the vulnerability.
- **Vulnerabilities Without Available Fixlets** - A list of vulnerabilities that do not have an available Fixlet for remediation.
- **Vulnerability Discrepancies** - A list of vulnerabilities where the scanning system identifies the issue, but BigFix does not see an applicable remediation.

Reporting fixlet uses dynamic downloading. To download the report, ensure that specific URL is added in the DownloadWhitelist.txt:

- Tenable.io
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_PowerBI_Tenableio.tmp
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_Tableau_Tenableio.tmp

- Tenable.sc
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_PowerBI_Tenable.tmp
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_Tableau_Tenable.tmp
- Qualys
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_PowerBI_Qualys.tmp
  - http://software.bigfix.com/download/ivr/1.4/Dashboards_Tableau_Qualys.tmp

The location of the file on the BigFix server is:

```
C:\Program Files (x86)\BigFix Enterprise\BES Server\Mirror Server\Config
```

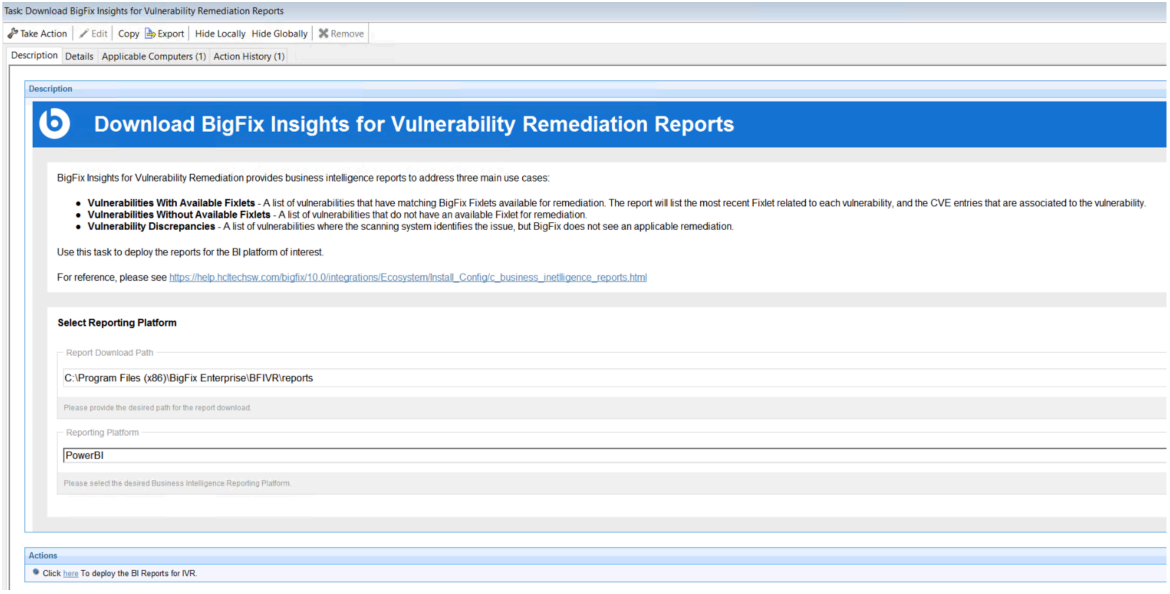
If the file does not exist, create a new one with the same name. The file should contain file formats such as the following:

http://127.0.0.1:52311/.*

http://software\.bigfix\.com/.*

Refer to the following link to find out more about **Dynamic download White-lists**.

Note: To use this task, you must have only one instance of IVR Dataflows service deployed in this environment.



Download BigFix Insights for Vulnerability Remediation Reports

BigFix Insights for Vulnerability Remediation provides business intelligence reports to address three main use cases:

- **Vulnerabilities With Available Fixlets** - A list of vulnerabilities that have matching BigFix Fixlets available for remediation. The report will list the most recent Fixlet related to each vulnerability, and the CVE entries that are associated to the vulnerability.
- **Vulnerabilities Without Available Fixlets** - A list of vulnerabilities that do not have an available Fixlet for remediation.
- **Vulnerability Discrepancies** - A list of vulnerabilities where the scanning system identifies the issue, but BigFix does not see an applicable remediation.

Use this task to deploy the reports for the BI platform of interest.

For reference, please see https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_business_inetlligence_reports.html

Select Reporting Platform

Report Download Path

C:\Program Files (x86)\BigFix Enterprise\BFIVR\reports

Please provide the desired path for the report download.

Reporting Platform

PowerBI

Please select the desired Business Intelligence Reporting Platform.

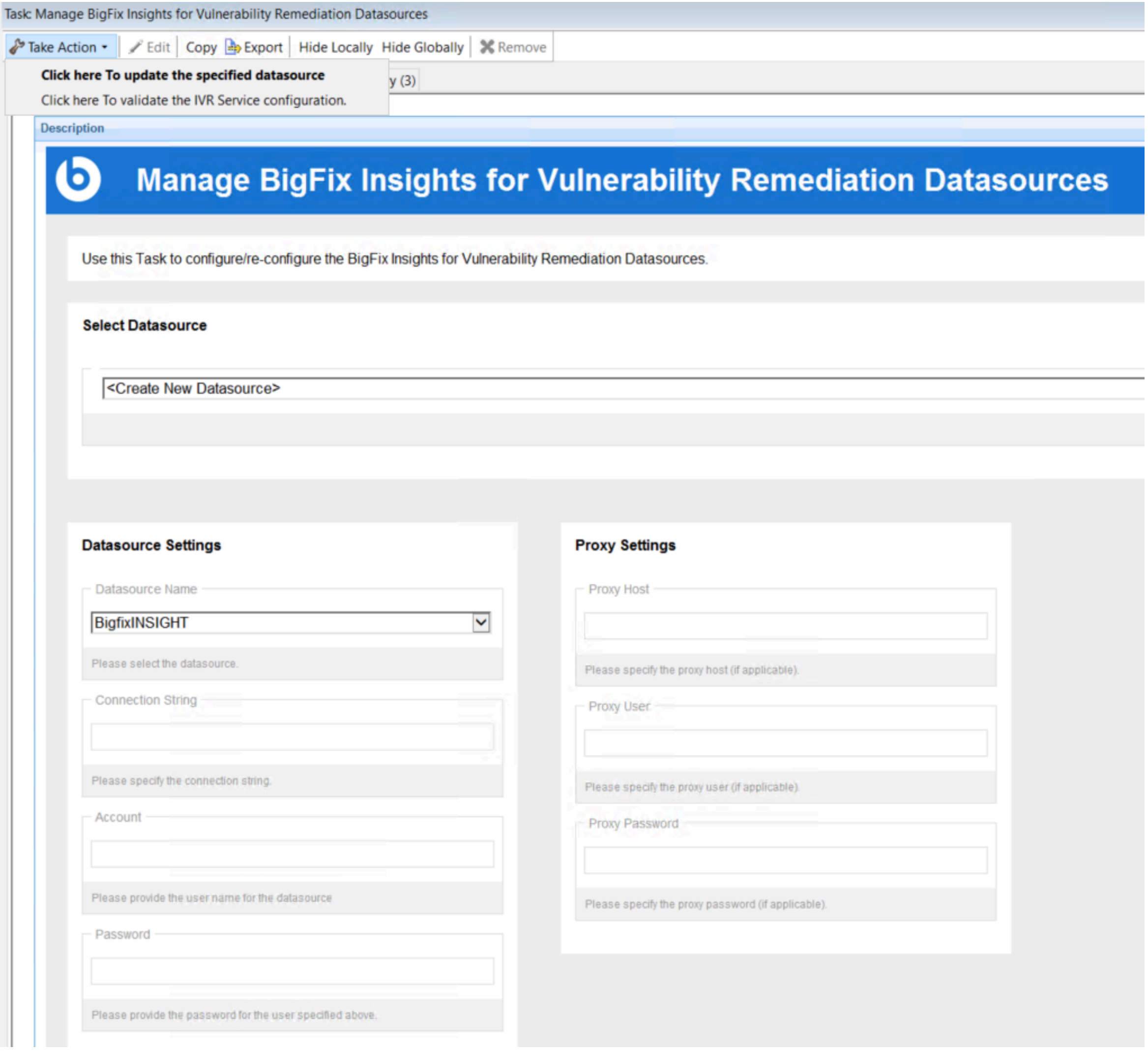
Actions

Click here To deploy the BI Reports for IVR.

Manage BigFix Insights for Vulnerability Remediation Datasources

You can use this task to update the specified datasouce or validate the IVR Service configuration. This task additionally provides option to specify proxy settings configuration for respective datasources.

Note: To use this task, you must have only one instance of IVR Dataflows service deployed in this environment.



Click here To update the specified datasource

Click here To validate the IVR Service configuration.

Manage BigFix Insights for Vulnerability Remediation Datasources

Use this Task to configure/re-configure the BigFix Insights for Vulnerability Remediation Datasources.

Select Datasource

<Create New Datasource>

Datasource Settings

Datasource Name: BigfixINSIGHT

Please select the datasource.

Connection String

Please specify the connection string.

Account

Please provide the user name for the datasource

Password

Please provide the password for the user specified above.

Proxy Settings

Proxy Host

Please specify the proxy host (if applicable).

Proxy User

Please specify the proxy user (if applicable).

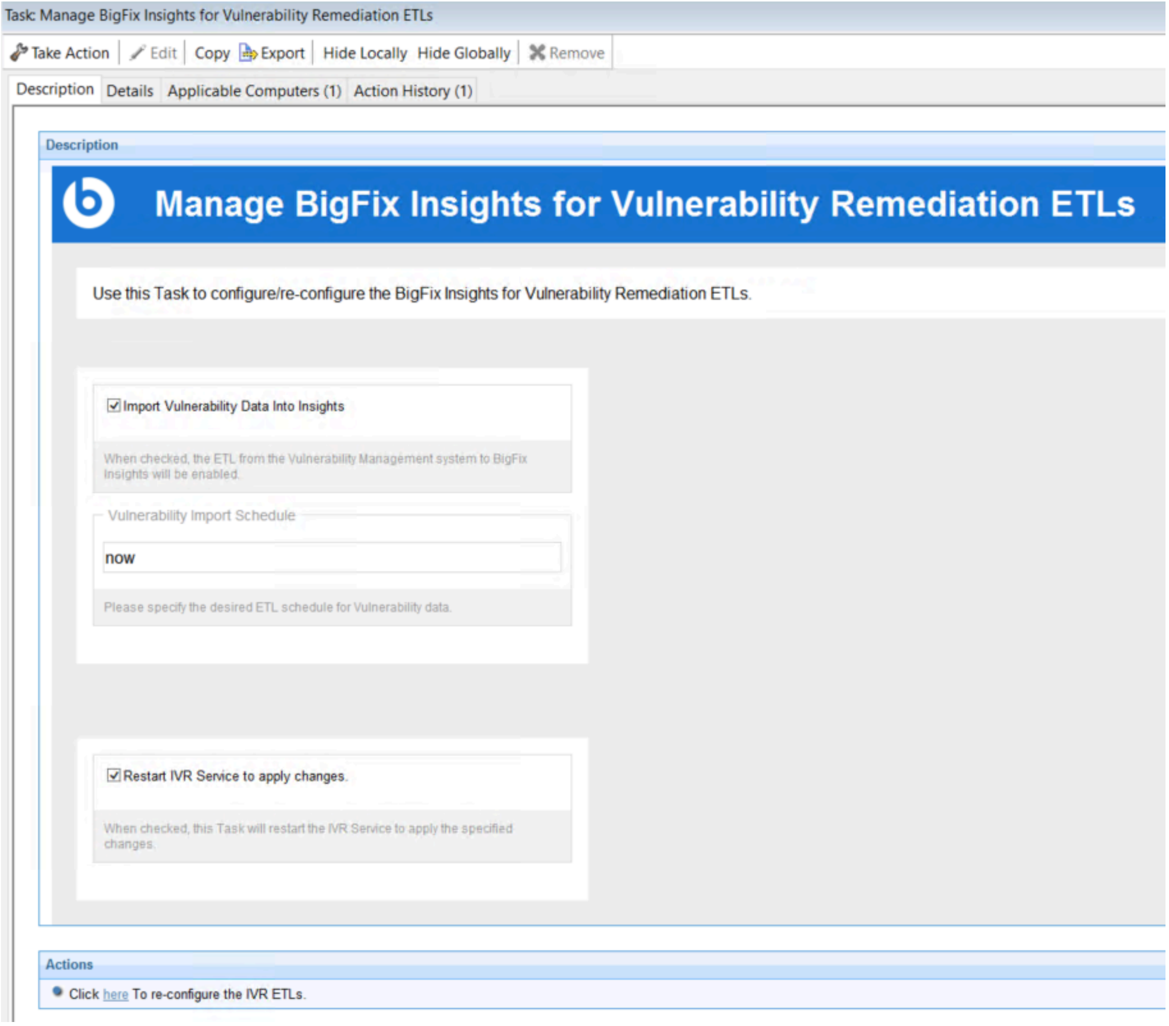
Proxy Password

Please specify the proxy password (if applicable).

Manage BigFix Insights for Vulnerability Remediation ETLs

Use this task to configure/re-configure the BigFix Insights for Vulnerability Remediation ETLs. You can also use this fixlet to restart the IVR Service.

Note: To use this task, you must have only one instance of IVR Dataflows service deployed in this environment.



Manage BigFix Insights for Vulnerability Remediation ETLs

Use this Task to configure/re-configure the BigFix Insights for Vulnerability Remediation ETLs.

☑ Import Vulnerability Data Into Insights

When checked, the ETL from the Vulnerability Management system to BigFix Insights will be enabled.

Vulnerability Import Schedule: now

Please specify the desired ETL schedule for Vulnerability data.

☑ Restart IVR Service to apply changes.

When checked, this Task will restart the IVR Service to apply the specified changes.

Actions

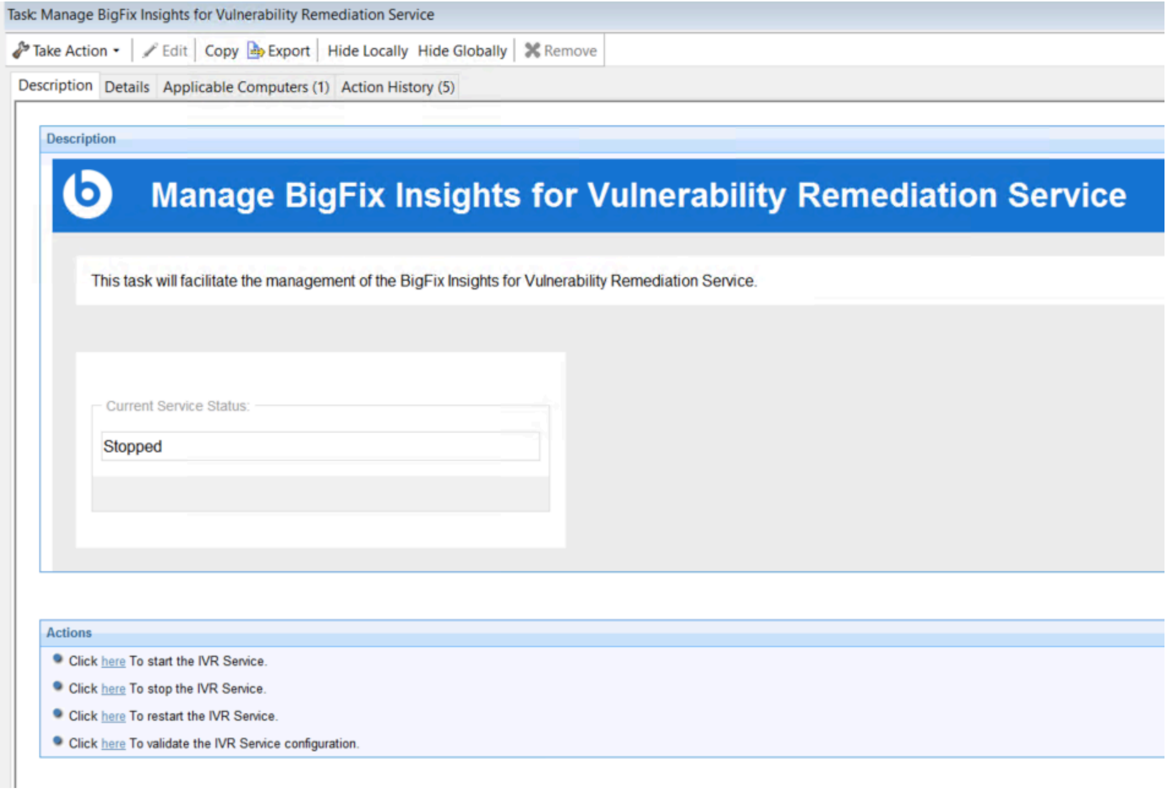
- Click here To re-configure the IVR ETLs.

Manage BigFix Insights for Vulnerability Remediation Service

This task facilitates the management of the BigFix Insights for Vulnerability Remediation Service. You can use this task to Start, Stop, Restart or validate the configuration of the IVR Service.

Note: It is always recommended to stop the service before making any update on datasource or ETL fixlet to the already deployed service and then restart the service to apply the latest changes.

Note: To use this task, you must have only one instance of IVR Dataflows service deployed in this environment.



Manage BigFix Insights for Vulnerability Remediation Service

This task will facilitate the management of the BigFix Insights for Vulnerability Remediation Service.

Current Service Status:

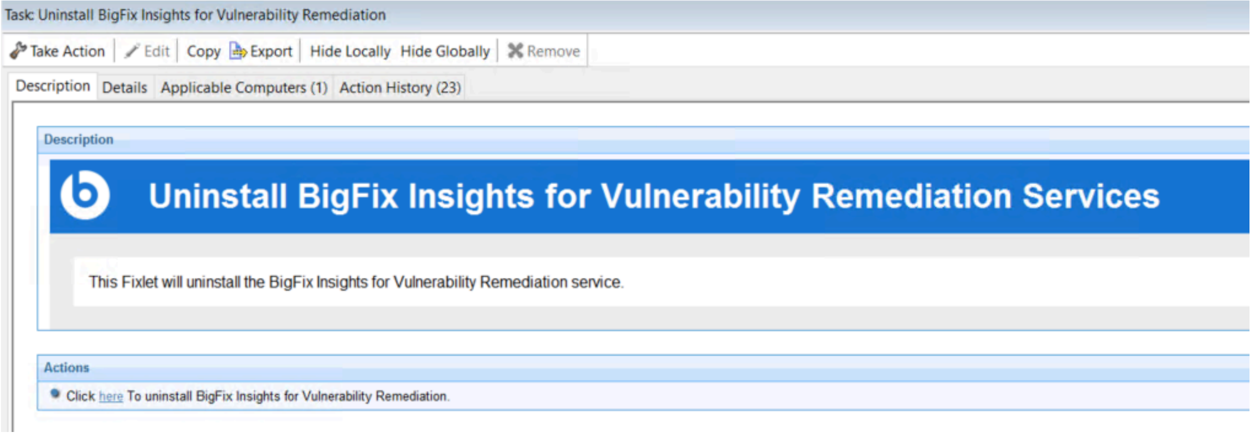
Stopped

Actions

- Click here To start the IVR Service.
- Click here To stop the IVR Service.
- Click here To restart the IVR Service.
- Click here To validate the IVR Service configuration.

Uninstall BigFix Insights for Vulnerability Remediation

This Fixlet uninstalls the BigFix Insights for Vulnerability Remediation service.



Uninstall BigFix Insights for Vulnerability Remediation Services

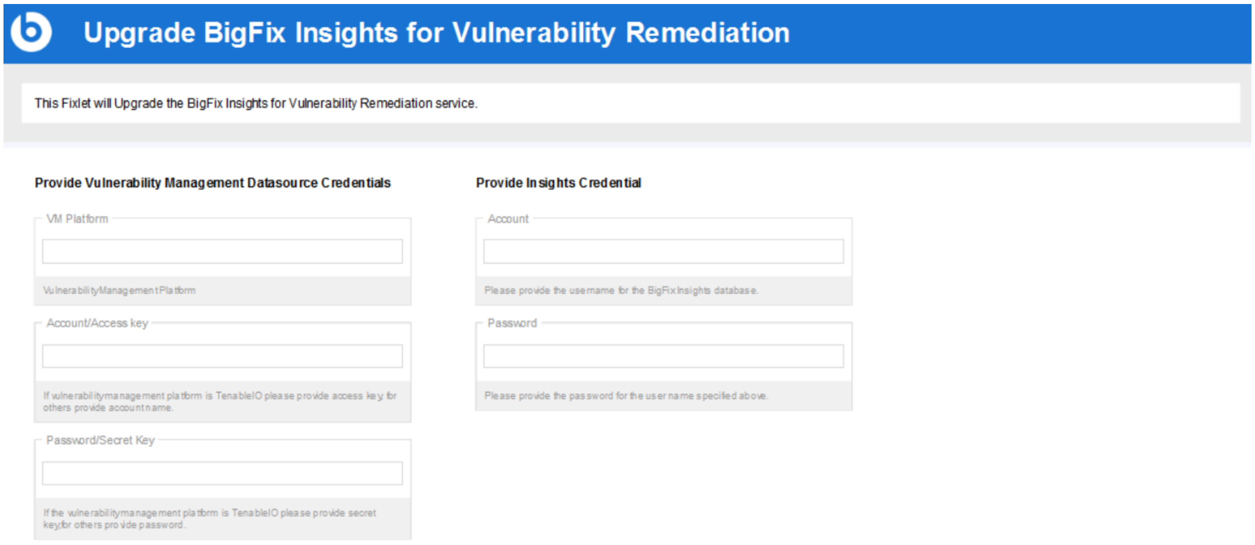
This Fixlet will uninstall the BigFix Insights for Vulnerability Remediation service.

Actions

- Click here To uninstall BigFix Insights for Vulnerability Remediation.

Upgrade BigFix Insights for Vunerability Remediation

The fixlet will upgrade the BigFix Insights for Vulnerability Remediation service to the most recent version. To initiate the upgrade, it is required to provide the BigFix Insights user credentials and vulnerability management datasource credentials.



Upgrade BigFix Insights for Vulnerability Remediation

This Fixlet will Upgrade the BigFix Insights for Vulnerability Remediation service.

Provide Vulnerability Management Datasource Credentials

VM Platform

VulnerabilityManagementPlatform

Account/Access key

If vulnerabilitymanagement platform is TenableIO please provide access key, for others provide accountname.

Password/Secret Key

If the vulnerabilitymanagement platform is TenableIO please provide secret key,for others provide password.

Provide Insights Credential

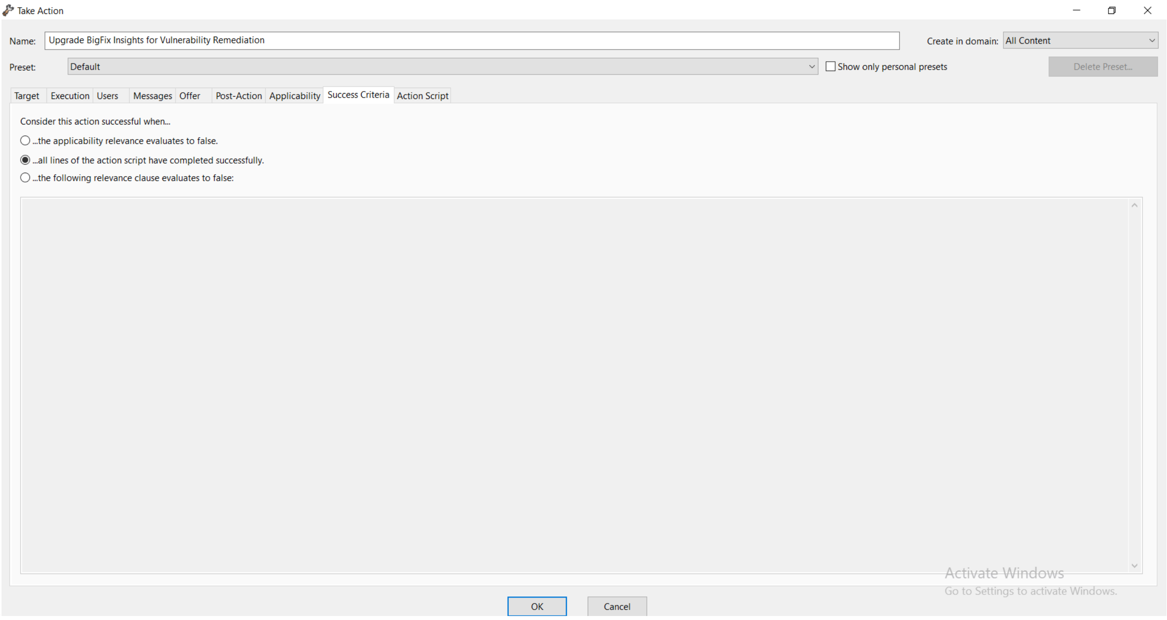
Account

Please provide the username for the BigFix Insights database.

Password

Please provide the password for the username specifed above.

Note: Before you install the Fixlet, go to **Success Criteria** tab and select **all lines of the action script have completed successfully**.



Take Action

Name: Upgrade BigFix Insights for Vulnerability Remediation

Create in domain: All Content

Preset: Default

□ Show only personal presets

Consider this action successful when...

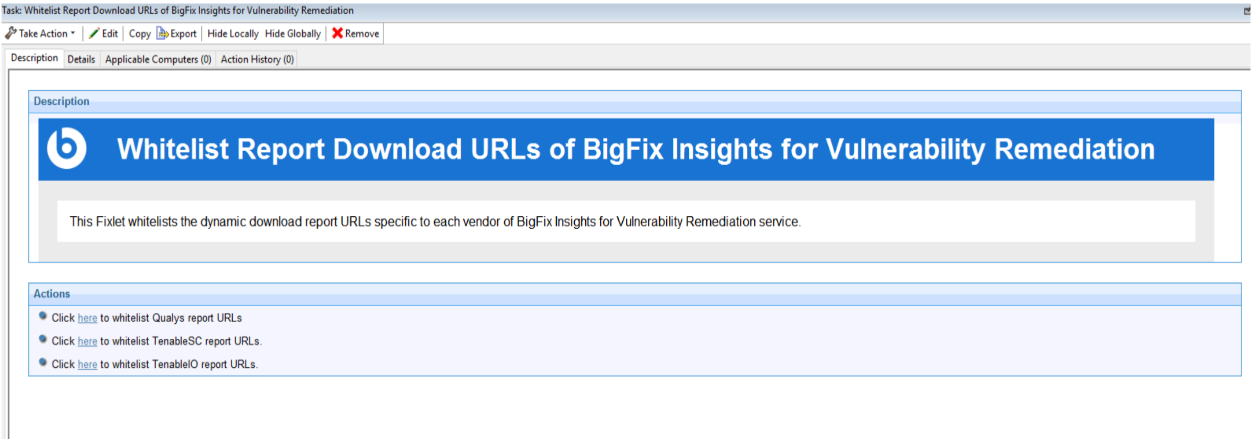
○ ...the applicability relevance evaluates to false.

● ...all lines of the action script have completed successfully.

○ ...the following relevance clause evaluates to false:

Whitelist Report Download URLs of BigFix Insights for Vulnerability Remediation

This Fixlet whitelists the dynamic download report URLs specific to each vendor of BigFix Insights for Vulnerability Remediation service.



Whitelist Report Download URLs of BigFix Insights for Vulnerability Remediation

This Fixlet whitelists the dynamic download report URLs specific to each vendor of BigFix Insights for Vulnerability Remediation service.

- Click here to whitelist Qualys report URLs
- Click here to whitelist TenableSC report URLs.
- Click here to whitelist TenableIO report URLs.

Chapter 7. Updating and validating the IVR configuration file

You can update and validate the IVR configuration.

Note: Configuration-file changes remove all IVR data that is associated with the current data flow configuration (from which a hash is generated). Additionally, all data that is not associated with existing data flow configurations are removed. For more information, see the PurgeFindingsOnExecutionOfDataflow setting.

Updating the configuration file

1. Log in to the target server.
2. Go to the product installation directory.
3. Open the `DataFlowsConfig.xml` file in a text editor.
4. Update configuration. For more information, see Configuration Settings.

Validating the configuration file

1. Open CLI (Command Line Interface) and run the `BFIVR.exe --ValidateConfiguration` command.
2. Restart BigFix Insights for Vulnerability Remediation to import the new configuration. On successful completion, the message, *Configuration verified successfully* appears.

Chapter 8. Updating IVR credentials

You can update the IVR credentials.

1. Open the command-line interface (CLI) and run the BFIVR.exe --ProvideCredentials command.
2. Enter a username/access key and password/secret key, as prompted.
3. To access the data source, enter the updated username/access key and password/secret key credentials.

After the update is complete, the following message is displayed: `The entered credentials are encrypted successfully.`

Chapter 9. Business Intelligence reports

Use this section to become familiar with Power BI and Tableau reports.

The reporting functionality of the IVR (BigFix Insights for Vulnerability Remediation) solution addresses the three main use cases for the application:

- **Vulnerabilities with Available Fixlets** - A list of vulnerabilities that have matching BigFix fixlets available for remediation. The report will list the most recent fixlet related to each vulnerability, and the CVE entries that are associated to the vulnerability
- **Vulnerabilities Without Available Fixlets** - A list of vulnerabilities that do not have an available fixlet for remediation
- **Vulnerability Discrepancies** - A list of vulnerabilities where the scanning system identifies the issue, but BigFix declares it resolved. This occurs primarily because of timing differences in the scan processes

The reports are produced in both Power BI (Desktop, optimized for BI Server, May 2020) and Tableau version 2020.4+.

Power BI reports

Tableau reports

Power BI reports

Use this section to become familiar with Power BI reports.

Power BI reports for:

- Qualys
- Tenable.io
- Tenable.sc

The reports are produced in Power BI (Desktop, optimized for BI Server, May 2020)

- Reporting differences: the functionality of the reports is nearly identical between Power BI and Tableau. This section details the differences between the reports.
- Navigation: each visualization is portrayed on the dashboard page. Visualizations that do not apply to your business process can be removed as necessary.

- Qualys Severity

  The Severity value is provided by Qualys to measure the relative security risk associated with the vulnerability. Factors included in this measure are:

  - Possible consequences
  - Complexity
  - Likelihood that the exploit will work under normal conditions

- Network location
- Privileges needed by the attacker
- Prevalence of affected software
- Existence of known attacks

In the IVR database, the information is stored in the vulnerabilities.severity column. The reporting aggregation tables return both the numerical score and a value (where applicable) corresponding to the following matrix:

Table 2.

Severity Value	Level Value
1	Minimal
2	Medium
3	Serious
4	Critical
5	Urgent

For more information regarding this topic from the vendor, please visit https://qualysguard.qualys.com/qwebhelp/fo_portal/knowledgebase/severity_levels.htm

- Tenable Severity

The Vulnerability Priority Rating (VPR) value is provided by Tenable to measure the relative security risk associated with the vulnerability. Factors included in this measure are:

- Vulnerability Age
- CVSSv3 Impact Score
- Exploit Code Maturity
- Product Coverage
- Threat Sources
- Threat Intensity
- Threat Recency

In the IVR database, the information is stored in the vulnerabilities.vendor_rating column. The reporting aggregation tables return both the numerical score and a value (where applicable) corresponding to the following matrix:

Table 3.

VPR Value	Level Value
9.0 – 10.0	Critical
7.0 – 8.9	High

VPR Value	Level Value
4.0 – 6.9	Medium
0.1 – 3.9	Low

For more information regarding this topic from the vendor, please visit https://docs.tenable.com/tenablesc/Content/RiskMetrics.htm

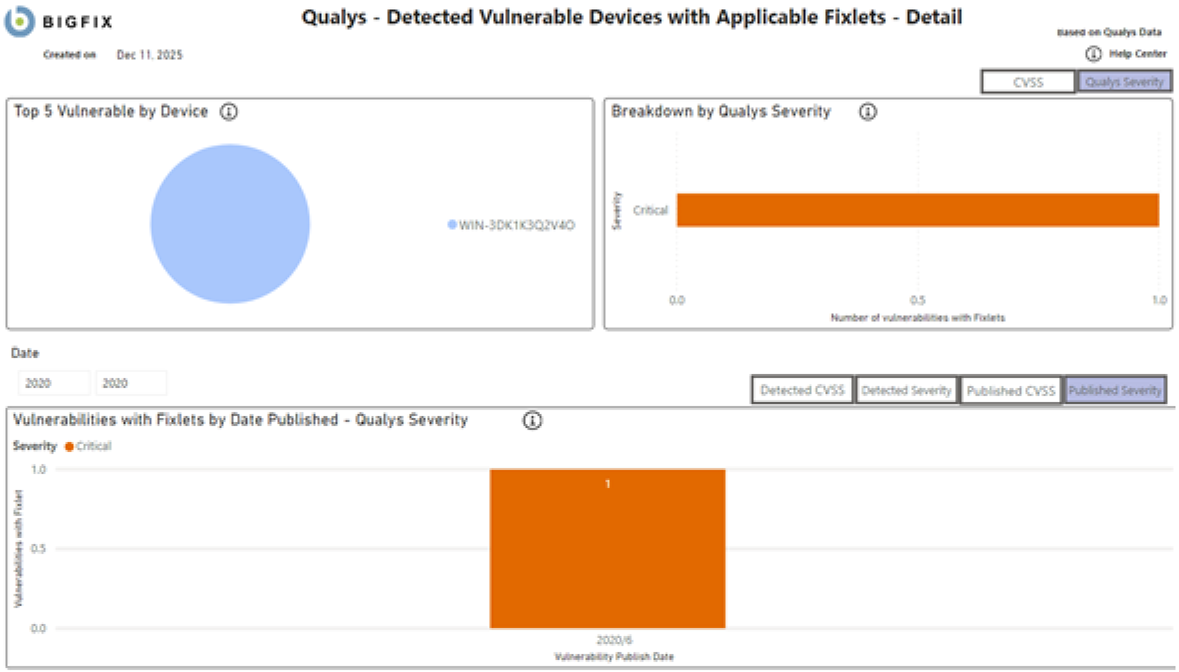
Power BI reports for Qualys

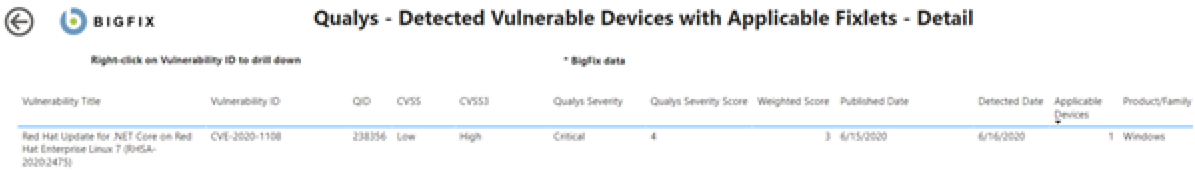
Use this section to become familiar with Power BI reports for Qualys.

Chart details:

- Vulnerability Title - vulnerability title
- Vulnerability ID - a unique identifier assigned to a vulnerability
- QID - Qualys ID. Unique identifier assigned to a vulnerability in the Qualys vulnerability database
- CVSS2 - Common Vulnerability Scoring System, version 2
- Qualys Severity - level of risk associated with a vulnerability.
- Qualys Severity Score - numerical value assigned to a vulnerability, representing the level of risk associated with that vulnerability. The severity score ranges from 1 to 5, with 5 being the highest severity.
- Weighted Score - value calculated based on cvss_base*applicable_computers as 'weighted score'
- Published Date - date when the information about a vulnerability was first available
- Detected Date - date when a vulnerability was first detected
- Appilcable Devices - devices that are affected by a vulnerability

Detected Vulnerabilities with Applicable Fixlets


BIGFIX
Created on Dec 11, 2025
Qualys - Detected Vulnerable Devices with Applicable Fixlets - Detail
Based on Qualys Data
Help Center
CVSS
Qualys Severity
Top 5 Vulnerable by Device
WIN-3DK1K3Q2V4O
Breakdown by Qualys Severity
Severity
Critical
0.0
0.5
1.0
Number of vulnerabilities with Fixlets
Date
2020
2020
Detected CVSS
Detected Severity
Published CVSS
Published Severity
Vulnerabilities with Fixlets by Date Published - Qualys Severity
Severity
Critical
1.0
0.5
0.0
Vulnerabilities with Fixlet
1
2020/6
Vulnerability Publish Date

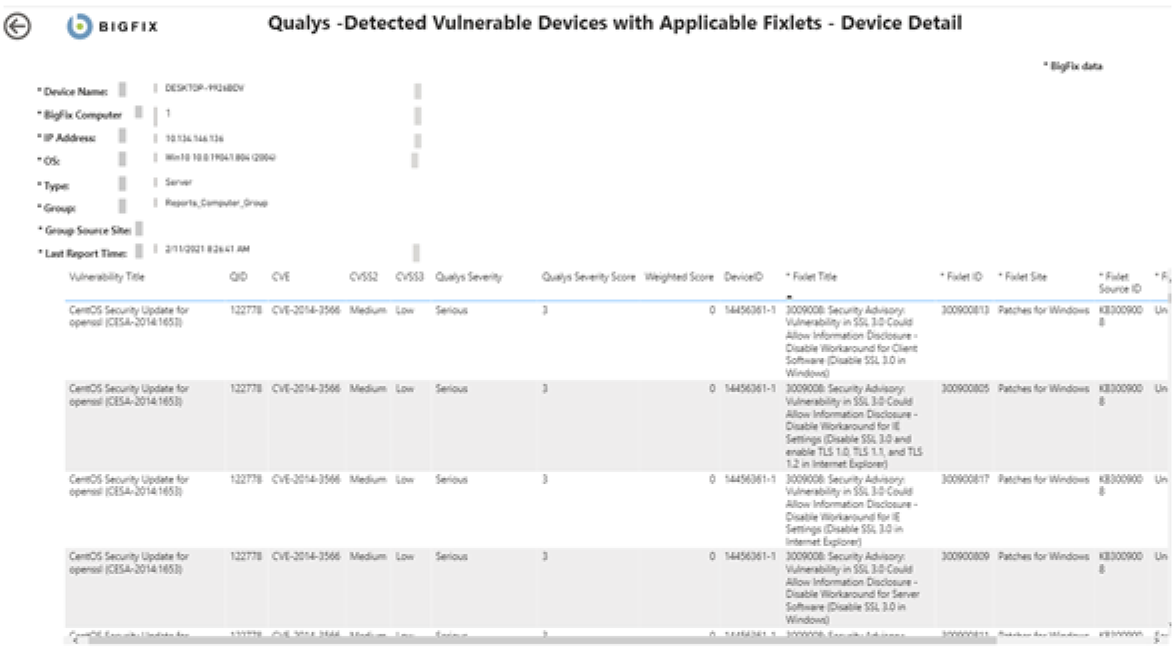


Qualys - Detected Vulnerable Devices with Applicable Fixlets - Detail

Right-click on Vulnerability ID to drill down

* BigFix data

Vulnerability Title	Vulnerability ID	QID	CVSS	CVSS3	Qualys Severity	Qualys Severity Score	Weighted Score	Published Date	Detected Date	Applicable Devices	Product/Family
Red Hat Update for .NET Core on Red Hat Enterprise Linux 7 (RHSA-2020:2475)	CVE-2020-1108	238356	Low	High	Critical	4	3	6/15/2020	6/16/2020	1	Windows

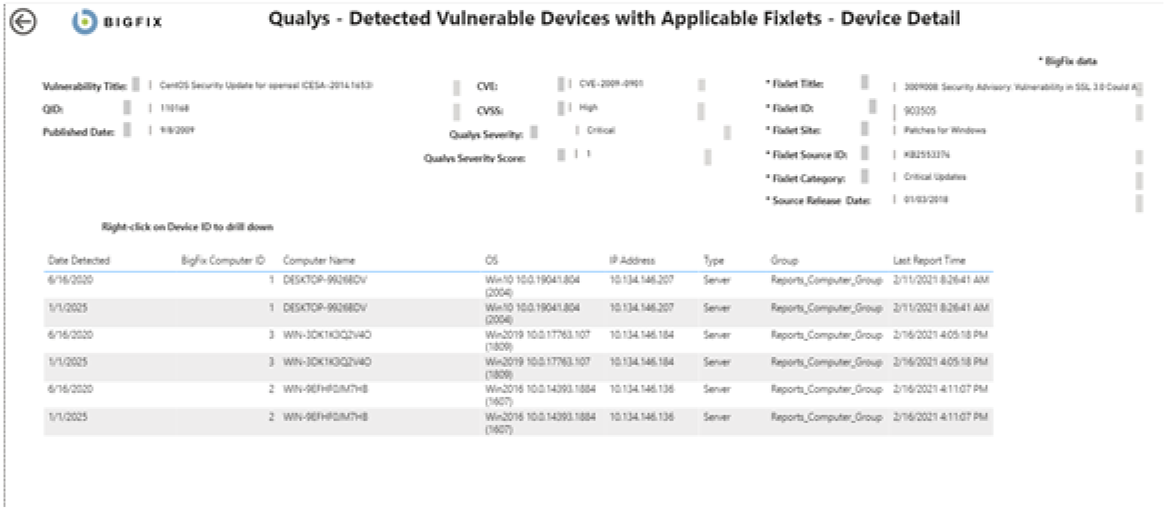


Qualys -Detected Vulnerable Devices with Applicable Fixlets - Device Detail

* BigFix data

* Device Name:	DESKTOP-99268DV
* BigFix Computer	1
* IP Address:	10.134.146.136
* OS:	Win10 10.0.19041.804 (2004)
* Type:	Server
* Group:	Reports_Computer_Group
* Group Source Site:	
* Last Report Time:	2/11/2021 8:26:41 AM

Vulnerability Title	QID	CVE	CVSS2	CVSS3	Qualys Severity	Qualys Severity Score	Weighted Score	DeviceID	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Source ID	* F
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for Client Software (Disable SSL 3.0 in Windows)	300900813	Patches for Windows	KB3009008	Un
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for IE Settings (Disable SSL 3.0 and enable TLS 1.0, TLS 1.1, and TLS 1.2 in Internet Explorer)	300900805	Patches for Windows	KB3009008	Un
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for IE Settings (Disable SSL 3.0 in Internet Explorer)	300900817	Patches for Windows	KB3009008	Un
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for Server Software (Disable SSL 3.0 in Windows)	300900809	Patches for Windows	KB3009008	Un
CentOS Security Update for	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory:	[illegible]	Patches for Windows	KB300900	[illegible]



Qualys - Detected Vulnerable Devices with Applicable Fixlets - Device Detail

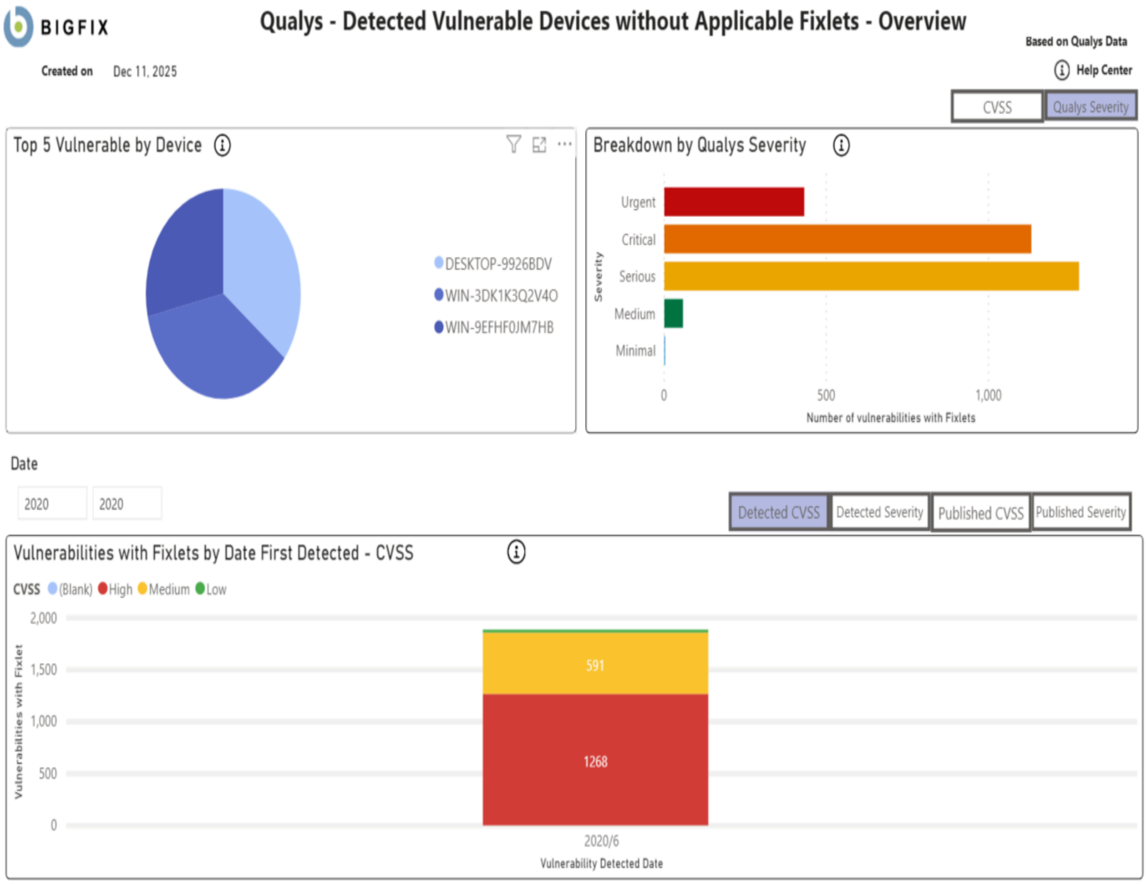
* BigFix data

Vulnerability Title:	CentOS Security Update for openssl (CESA-2014:1653)
QID:	110168
Published Date:	9/8/2009
CVE:	CVE-2009-0901
CVSS:	High
Qualys Severity:	Critical
Qualys Severity Score:	1
* Fixlet Title:	3009008: Security Advisory: Vulnerability in SSL 3.0 Could A
* Fixlet ID:	903505
* Fixlet Site:	Patches for Windows
* Fixlet Source ID:	KB2553376
* Fixlet Category:	Critical Updates
* Source Release Date:	01/03/2018

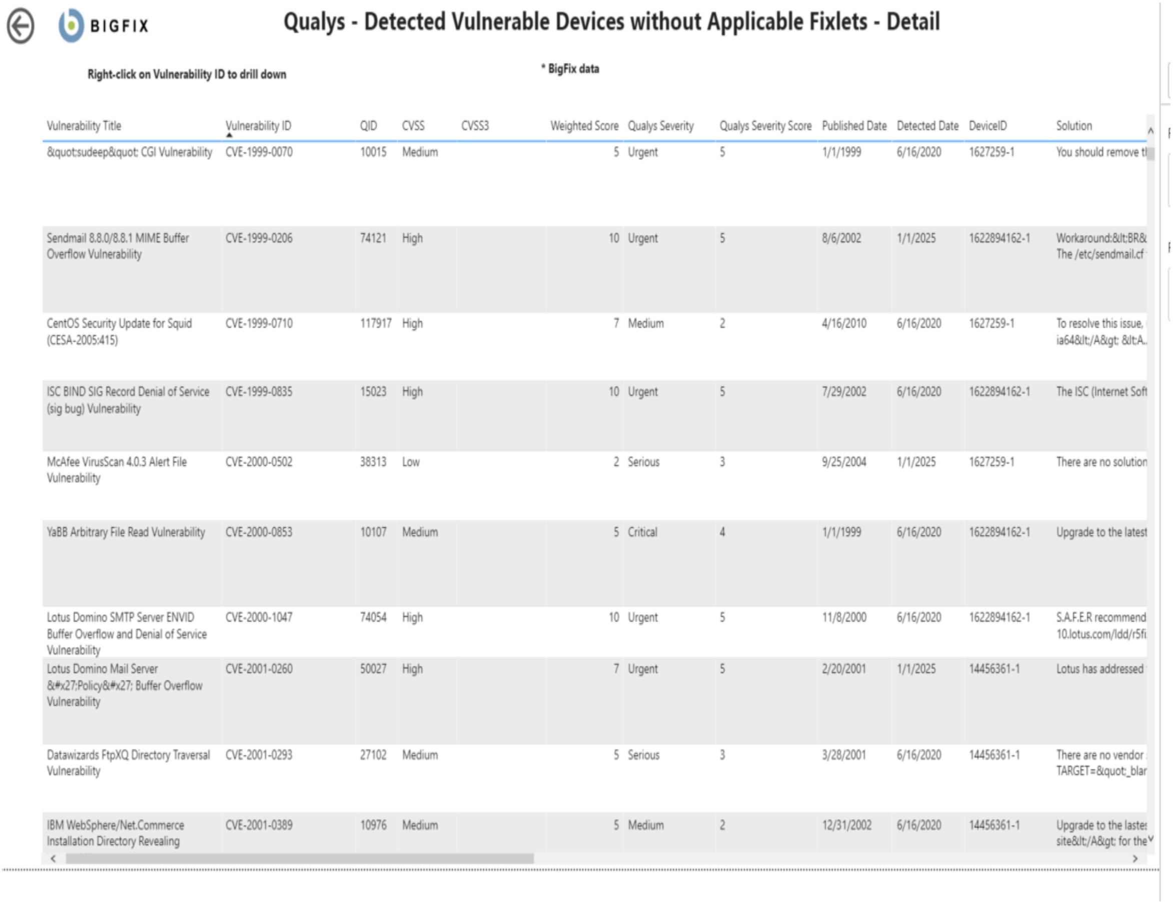
Right-click on Device ID to drill down

Date Detected	BigFix Computer ID	Computer Name	OS	IP Address	Type	Group	Last Report Time
6/16/2020	1	DESKTOP-99268DV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	Reports_Computer_Group	2/11/2021 8:26:41 AM
1/1/2025	1	DESKTOP-99268DV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	Reports_Computer_Group	2/11/2021 8:26:41 AM
6/16/2020	3	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	Reports_Computer_Group	2/16/2021 4:05:18 PM
1/1/2025	3	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	Reports_Computer_Group	2/16/2021 4:05:18 PM
6/16/2020	2	WIN-9EFHF0JM7H8	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	Reports_Computer_Group	2/16/2021 4:11:07 PM
1/1/2025	2	WIN-9EFHF0JM7H8	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	Reports_Computer_Group	2/16/2021 4:11:07 PM

Detected Vulnerabilities without Available Fixlets


BIGFIX
Qualys - Detected Vulnerable Devices without Applicable Fixlets - Overview
Created on Dec 11, 2025
Based on Qualys Data
Help Center
CVSS
Qualys Severity
Top 5 Vulnerable by Device
DESKTOP-9926BDV
WIN-3DK1K3Q2V4O
WIN-9EFHF0JM7HB
Breakdown by Qualys Severity
Severity
Urgent
Critical
Serious
Medium
Minimal
0
500
1,000
Number of vulnerabilities with Fixlets
Date
2020
2020
Detected CVSS
Detected Severity
Published CVSS
Published Severity
Vulnerabilities with Fixlets by Date First Detected - CVSS
CVSS ● (Blank) ● High ● Medium ● Low
Vulnerabilities with Fixlet
2,000
1,500
1,000
500
0
591
1268
2020/6
Vulnerability Detected Date

-

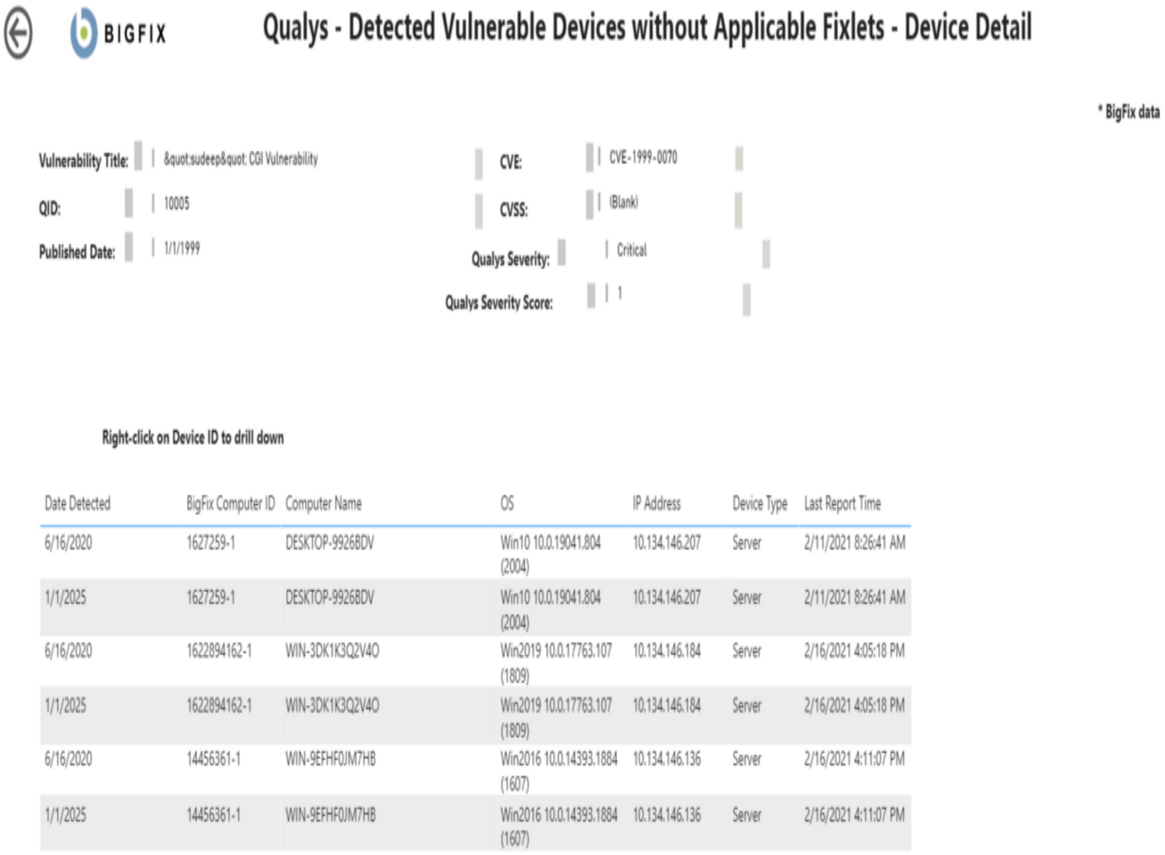


Qualys - Detected Vulnerable Devices without Applicable Fixlets - Detail

Right-click on Vulnerability ID to drill down

* BigFix data

Vulnerability Title	Vulnerability ID	QID	CVSS	CVSS3	Weighted Score	Qualys Severity	Qualys Severity Score	Published Date	Detected Date	DeviceID	Solution
&quot;sudeep&quot; CGI Vulnerability	CVE-1999-0070	10015	Medium		5	Urgent	5	1/1/1999	6/16/2020	1627259-1	You should remove t
Sendmail 8.8.0/8.8.1 MIME Buffer Overflow Vulnerability	CVE-1999-0206	74121	High		10	Urgent	5	8/6/2002	1/1/2025	1622894162-1	Workaround:<BR& The /etc/sendmail.cf
CentOS Security Update for Squid (CESA-2005:415)	CVE-1999-0710	117917	High		7	Medium	2	4/16/2010	6/16/2020	1627259-1	To resolve this issue, ia64</A> <A...
ISC BIND SIG Record Denial of Service (sig bug) Vulnerability	CVE-1999-0835	15023	High		10	Urgent	5	7/29/2002	6/16/2020	1622894162-1	The ISC (Internet Soft
McAfee VirusScan 4.0.3 Alert File Vulnerability	CVE-2000-0502	38313	Low		2	Serious	3	9/25/2004	1/1/2025	1627259-1	There are no solution
YaBB Arbitrary File Read Vulnerability	CVE-2000-0853	10107	Medium		5	Critical	4	1/1/1999	6/16/2020	1622894162-1	Upgrade to the latest
Lotus Domino SMTP Server ENVID Buffer Overflow and Denial of Service Vulnerability	CVE-2000-1047	74054	High		10	Urgent	5	11/8/2000	6/16/2020	1622894162-1	S.A.F.E.R recommend 10.lotus.com/ldd/r5fi
Lotus Domino Mail Server &#x27;Policy&#x27; Buffer Overflow Vulnerability	CVE-2001-0260	50027	High		7	Urgent	5	2/20/2001	1/1/2025	14456361-1	Lotus has addressed
Datawizards FtpXQ Directory Traversal Vulnerability	CVE-2001-0293	27102	Medium		5	Serious	3	3/28/2001	6/16/2020	14456361-1	There are no vendor TARGET=&quot;_blar
IBM WebSphere/Net.Commerce Installation Directory Revealing	CVE-2001-0389	10976	Medium		5	Medium	2	12/31/2002	6/16/2020	14456361-1	Upgrade to the lates site</A> for the



Qualys - Detected Vulnerable Devices without Applicable Fixlets - Device Detail

* BigFix data

Vulnerability Title: &quot;sudeep&quot; CGI Vulnerability

QID: 10005

Published Date: 1/1/1999

CVE: CVE-1999-0070

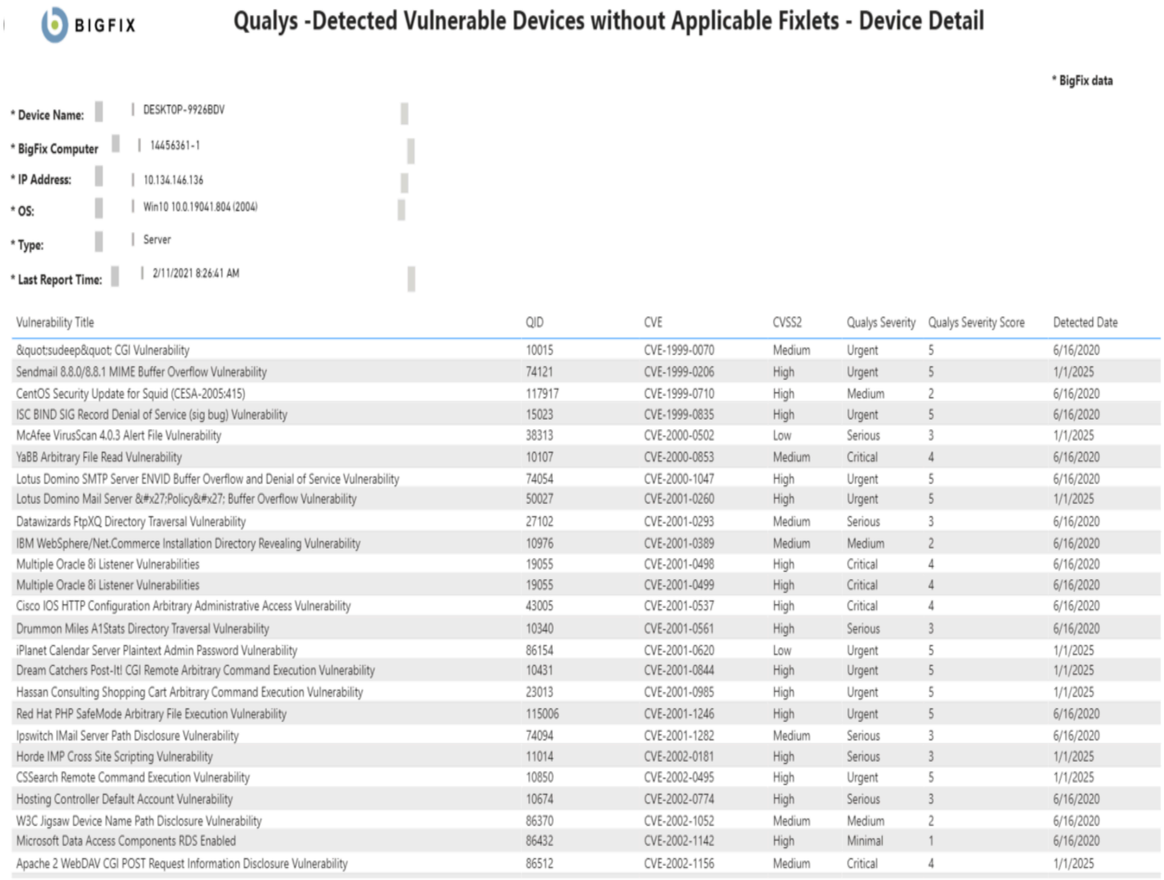
CVSS: (Blank)

Qualys Severity: Critical

Qualys Severity Score: 1

Right-click on Device ID to drill down

Date Detected	BigFix Computer ID	Computer Name	OS	IP Address	Device Type	Last Report Time
6/16/2020	1627259-1	DESKTOP-9926BDV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	2/11/2021 8:26:41 AM
1/1/2025	1627259-1	DESKTOP-9926BDV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	2/11/2021 8:26:41 AM
6/16/2020	1622894162-1	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	2/16/2021 4:05:18 PM
1/1/2025	1622894162-1	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	2/16/2021 4:05:18 PM
6/16/2020	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	2/16/2021 4:11:07 PM
1/1/2025	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	2/16/2021 4:11:07 PM



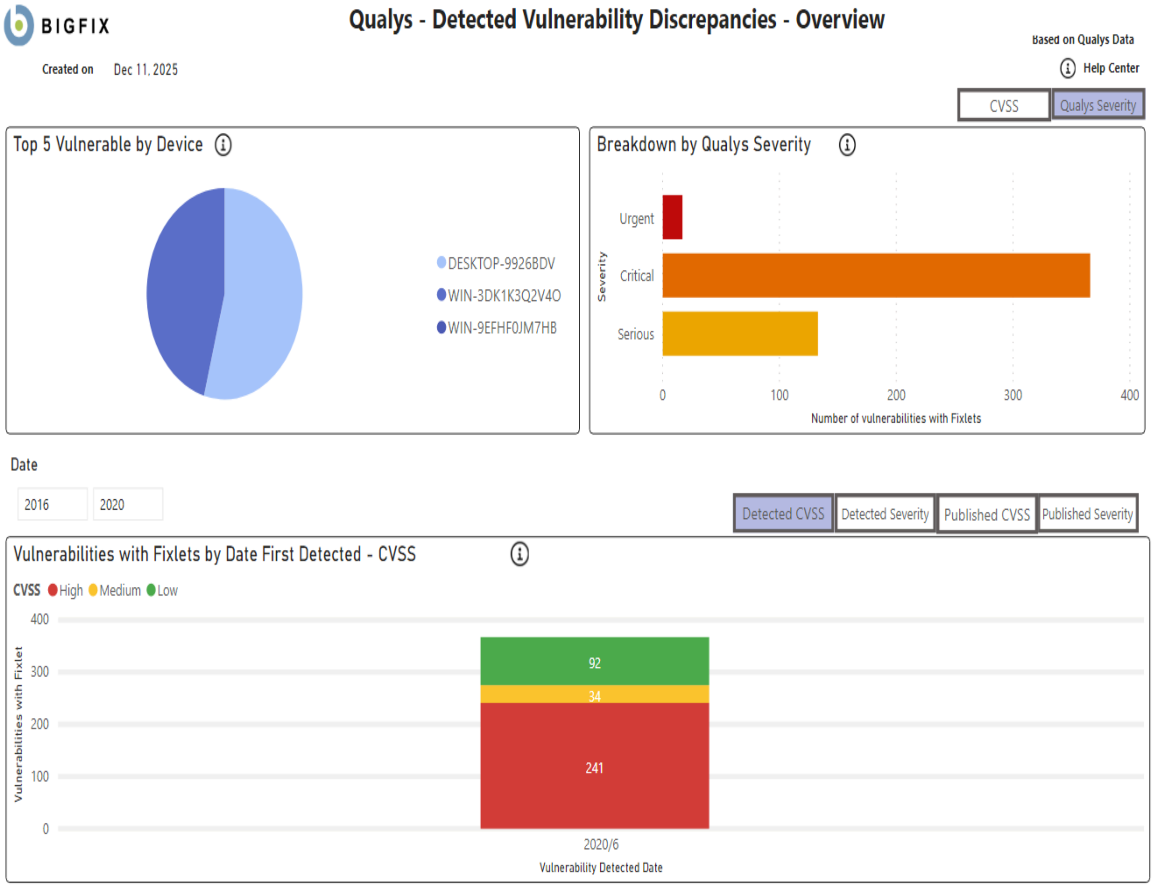
Qualys -Detected Vulnerable Devices without Applicable Fixlets - Device Detail

* BigFix data

* Device Name:	DESKTOP-9926BDV
* BigFix Computer	14456361-1
* IP Address:	10.134.146.136
* OS:	Win10 10.0.19041.804 (2004)
* Type:	Server
* Last Report Time:	2/11/2021 8:26:41 AM

Vulnerability Title	QID	CVE	CVSS2	Qualys Severity	Qualys Severity Score	Detected Date
&quot;sudeep&quot; CGI Vulnerability	10015	CVE-1999-0070	Medium	Urgent	5	6/16/2020
Sendmail 8.8.0/8.8.1 MIME Buffer Overflow Vulnerability	74121	CVE-1999-0206	High	Urgent	5	1/1/2025
CentOS Security Update for Squid (CESA-2005:415)	117917	CVE-1999-0710	High	Medium	2	6/16/2020
ISC BIND SIG Record Denial of Service (sig bug) Vulnerability	15023	CVE-1999-0835	High	Urgent	5	6/16/2020
McAfee VirusScan 4.0.3 Alert File Vulnerability	38313	CVE-2000-0502	Low	Serious	3	1/1/2025
YaBB Arbitrary File Read Vulnerability	10107	CVE-2000-0853	Medium	Critical	4	6/16/2020
Lotus Domino SMTP Server ENVID Buffer Overflow and Denial of Service Vulnerability	74054	CVE-2000-1047	High	Urgent	5	6/16/2020
Lotus Domino Mail Server &#x27;Policy&#x27; Buffer Overflow Vulnerability	50027	CVE-2001-0260	High	Urgent	5	1/1/2025
Datawizards FtpXQ Directory Traversal Vulnerability	27102	CVE-2001-0293	Medium	Serious	3	6/16/2020
IBM WebSphere/Net.Commerce Installation Directory Revealing Vulnerability	10976	CVE-2001-0389	Medium	Medium	2	6/16/2020
Multiple Oracle 8i Listener Vulnerabilities	19055	CVE-2001-0498	High	Critical	4	6/16/2020
Multiple Oracle 8i Listener Vulnerabilities	19055	CVE-2001-0499	High	Critical	4	6/16/2020
Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability	43005	CVE-2001-0537	High	Critical	4	6/16/2020
Drummon Miles A1Stats Directory Traversal Vulnerability	10340	CVE-2001-0561	High	Serious	3	6/16/2020
iPlanet Calendar Server Plaintext Admin Password Vulnerability	86154	CVE-2001-0620	Low	Urgent	5	1/1/2025
Dream Catchers Post-It! CGI Remote Arbitrary Command Execution Vulnerability	10431	CVE-2001-0844	High	Urgent	5	1/1/2025
Hassan Consulting Shopping Cart Arbitrary Command Execution Vulnerability	23013	CVE-2001-0985	High	Urgent	5	1/1/2025
Red Hat PHP SafeMode Arbitrary File Execution Vulnerability	115006	CVE-2001-1246	High	Urgent	5	6/16/2020
Ipswitch IMail Server Path Disclosure Vulnerability	74094	CVE-2001-1282	Medium	Serious	3	6/16/2020
Horde IMP Cross Site Scripting Vulnerability	11014	CVE-2002-0181	High	Serious	3	1/1/2025
CSSearch Remote Command Execution Vulnerability	10850	CVE-2002-0495	High	Urgent	5	1/1/2025
Hosting Controller Default Account Vulnerability	10674	CVE-2002-0774	High	Serious	3	6/16/2020
W3C Jigsaw Device Name Path Disclosure Vulnerability	86370	CVE-2002-1052	Medium	Medium	2	6/16/2020
Microsoft Data Access Components RDS Enabled	86432	CVE-2002-1142	High	Minimal	1	6/16/2020
Apache 2 WebDAV CGI POST Request Information Disclosure Vulnerability	86512	CVE-2002-1156	Medium	Critical	4	1/1/2025

Vulnerability Discrepancies



BIGFIX

Qualys - Detected Vulnerability Discrepancies - Overview

Created on Dec 11, 2025

Based on Qualys Data

Help Center

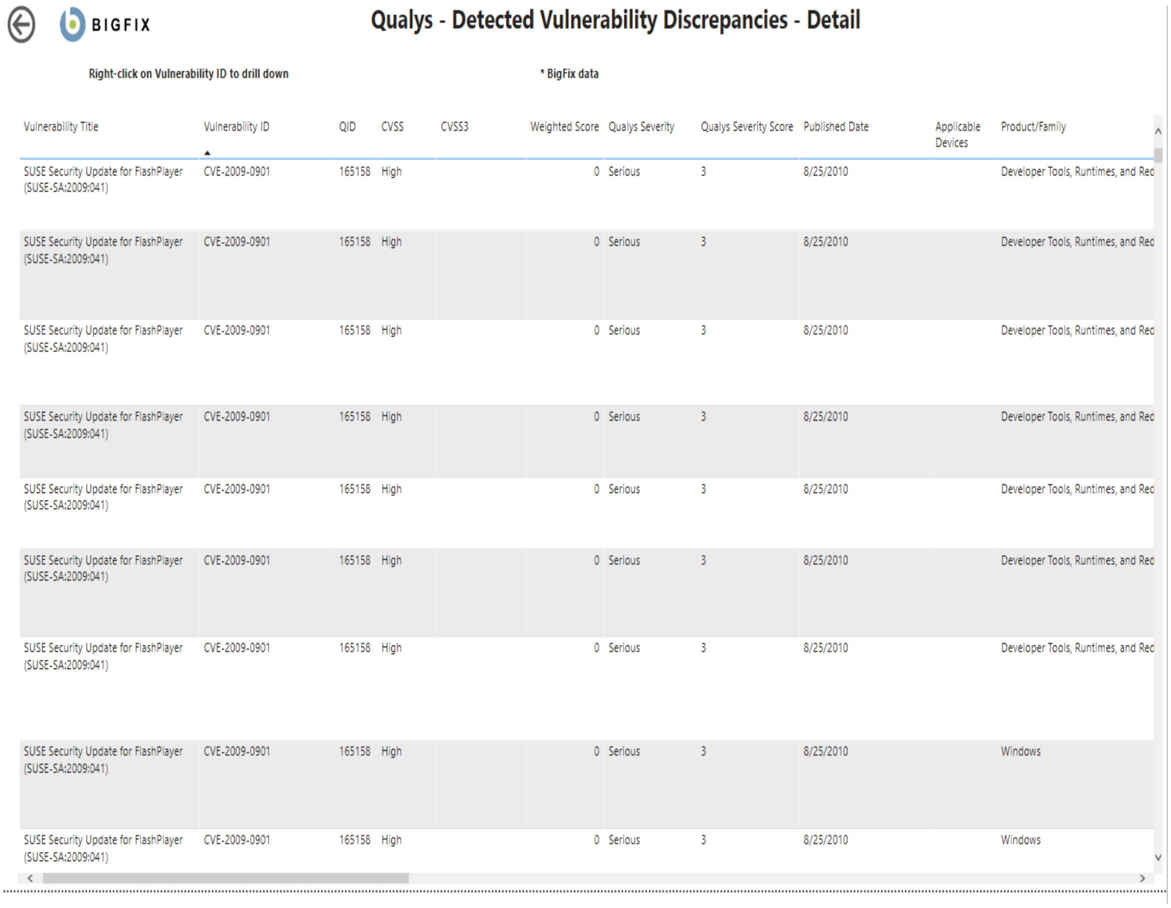
Top 5 Vulnerable by Device

Breakdown by Qualys Severity

Date

2016 2020

Vulnerabilities with Fixlets by Date First Detected - CVSS

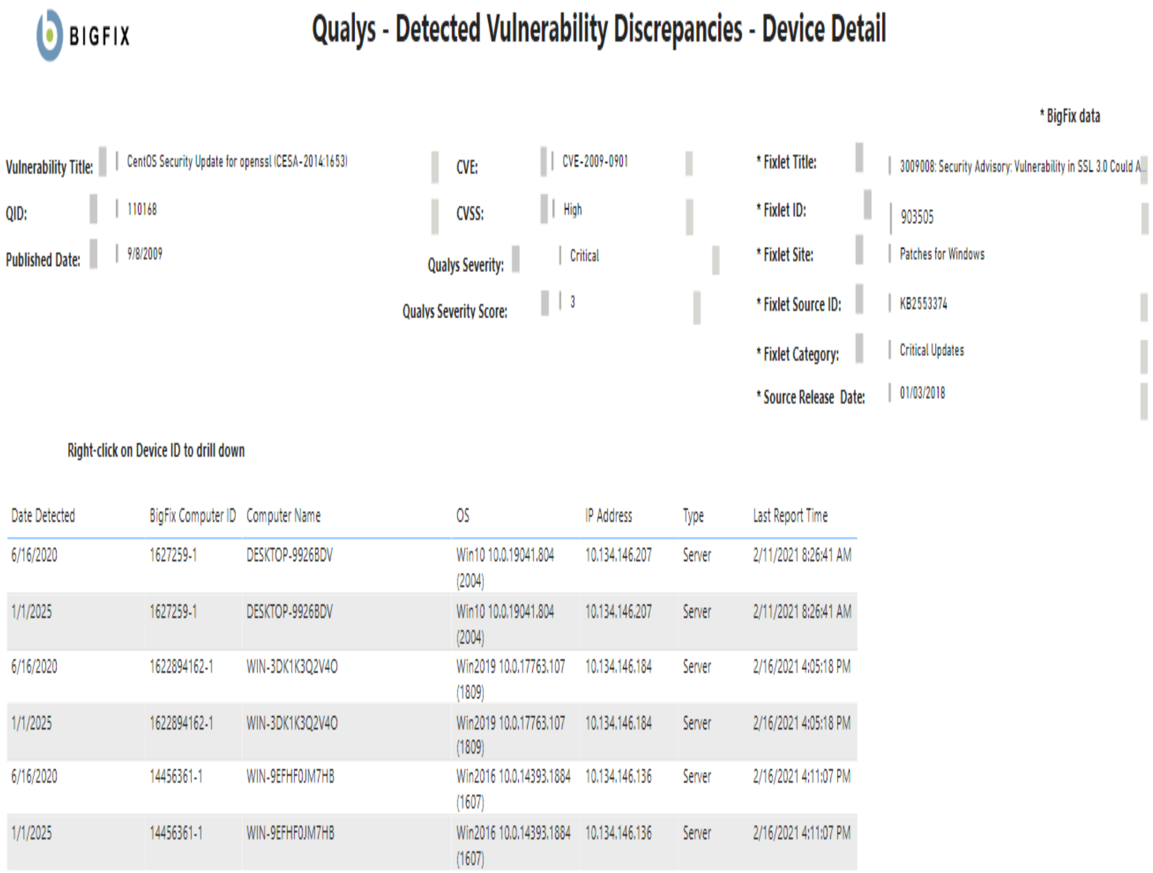


Qualys - Detected Vulnerability Discrepancies - Detail

Right-click on Vulnerability ID to drill down

* BigFix data

Vulnerability Title	Vulnerability ID	QID	CVSS	CVSS3	Weighted Score	Qualys Severity	Qualys Severity Score	Published Date	Applicable Devices	Product/Family
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Developer Tools, Runtimes, and Red
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Windows
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	CVE-2009-0901	165158	High		0	Serious	3	8/25/2010		Windows



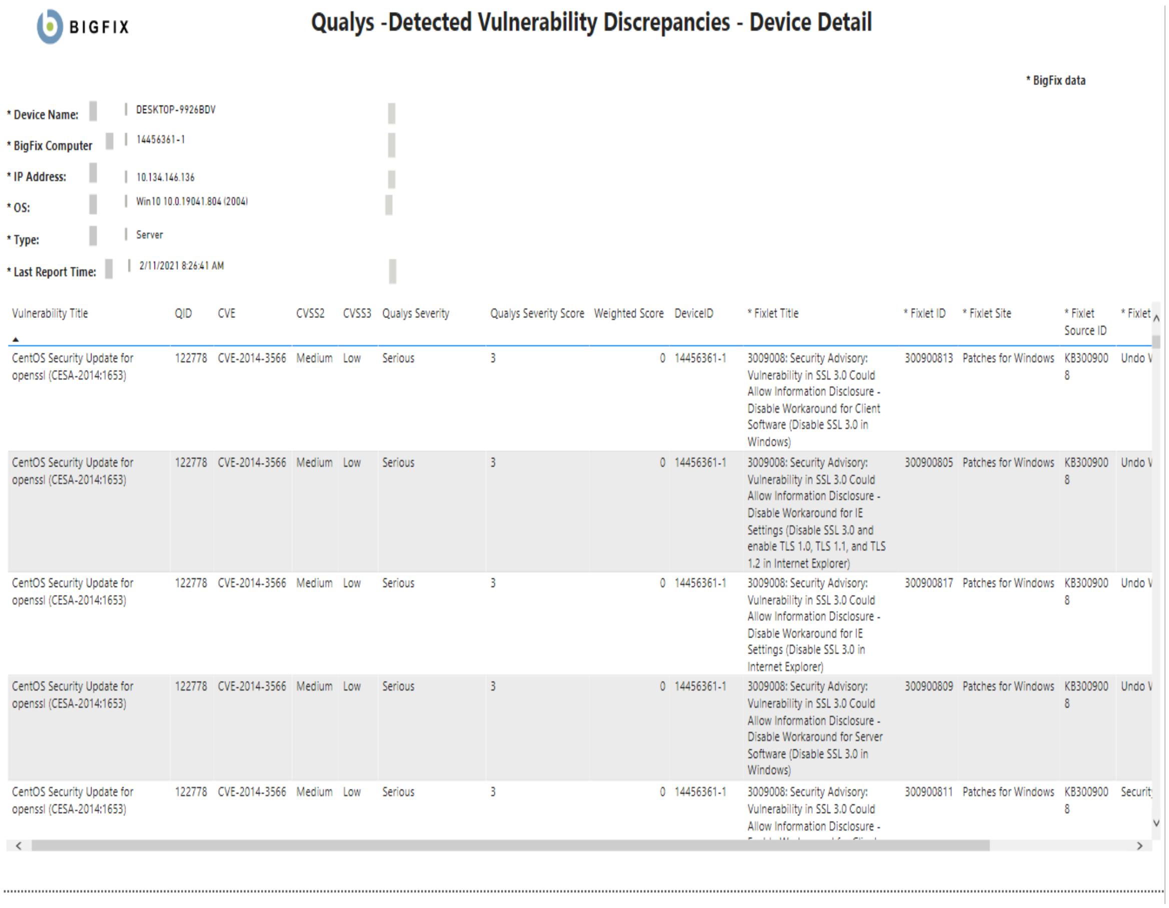
Qualys - Detected Vulnerability Discrepancies - Device Detail

* BigFix data

Vulnerability Title:	CentOS Security Update for openssl (CESA-2014:1653)	CVE:	CVE-2009-0901	* Fixlet Title:	3009008: Security Advisory: Vulnerability in SSL 3.0 Could A...
QID:	110168	CVSS:	High	* Fixlet ID:	903505
Published Date:	9/8/2009	Qualys Severity:	Critical	* Fixlet Site:	Patches for Windows
		Qualys Severity Score:	3	* Fixlet Source ID:	KB2553374
				* Fixlet Category:	Critical Updates
				* Source Release Date:	01/03/2018

Right-click on Device ID to drill down

Date Detected	BigFix Computer ID	Computer Name	OS	IP Address	Type	Last Report Time
6/16/2020	1627259-1	DESKTOP-9926BDV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	2/11/2021 8:26:41 AM
1/1/2025	1627259-1	DESKTOP-9926BDV	Win10 10.0.19041.804 (2004)	10.134.146.207	Server	2/11/2021 8:26:41 AM
6/16/2020	1622894162-1	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	2/16/2021 4:05:18 PM
1/1/2025	1622894162-1	WIN-3DK1K3Q2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	2/16/2021 4:05:18 PM
6/16/2020	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	2/16/2021 4:11:07 PM
1/1/2025	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 (1607)	10.134.146.136	Server	2/16/2021 4:11:07 PM



Qualys -Detected Vulnerability Discrepancies - Device Detail

* BigFix data

* Device Name: DESKTOP-9926BDV

* BigFix Computer 14456361-1

* IP Address: 10.134.146.136

* OS: Win10 10.0.19041.804 (2004)

* Type: Server

* Last Report Time: 2/11/2021 8:26:41 AM

Vulnerability Title	QID	CVE	CVSS2	CVSS3	Qualys Severity	Qualys Severity Score	Weighted Score	DeviceID	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Source ID	* Fixlet
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for Client Software (Disable SSL 3.0 in Windows)	300900813	Patches for Windows	KB3009008	Undo V
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for IE Settings (Disable SSL 3.0 and enable TLS 1.0, TLS 1.1, and TLS 1.2 in Internet Explorer)	300900805	Patches for Windows	KB3009008	Undo V
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for IE Settings (Disable SSL 3.0 in Internet Explorer)	300900817	Patches for Windows	KB3009008	Undo V
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for Server Software (Disable SSL 3.0 in Windows)	300900809	Patches for Windows	KB3009008	Undo V
CentOS Security Update for openssl (CESA-2014:1653)	122778	CVE-2014-3566	Medium	Low	Serious	3	0	14456361-1	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure -	300900811	Patches for Windows	KB3009008	Securit

Power BI reports for Tenable.io

Use this section to become familiar with Power BI reports for Tenable.io

BigFix Insights for Vulnerability Remediation can consume vulnerability data from Tenable.io. With Tenable Lumin available, BigFix Insights for Vulnerability Remediation also consumes asset prioritization data:

- Asset Criticality Rating (ACR): 1-10 rating that represents the asset's relative criticality based on device type, device purpose, and network location/proximity to the Internet.
- Asset Exposure Score (AES): A metric that combines ACR & VPR (Vulnerability Priority Rating) into a single score to represent an asset's relative exposure.

Refer to the link for more information: Lumin Metrics

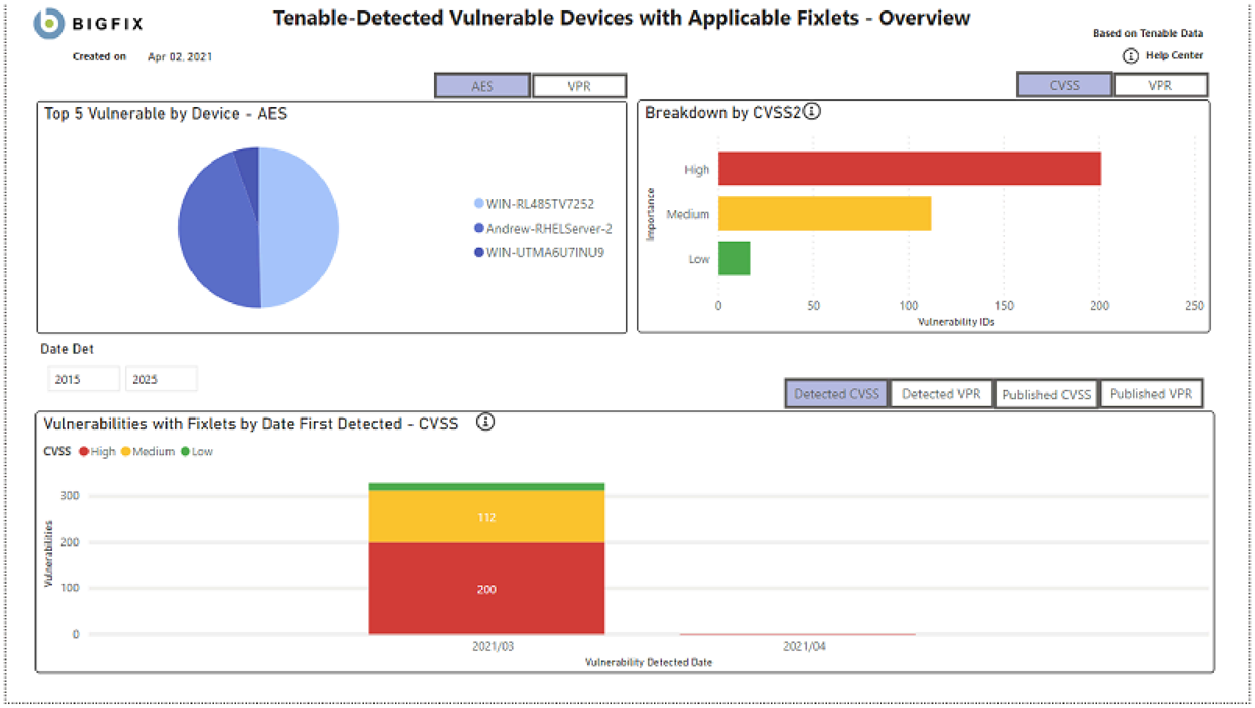
Additionally, uniquely for Tenable.io, BigFix sends its endpoint asset data to Tenable.io to give it visibility into potentially unmanaged assets.

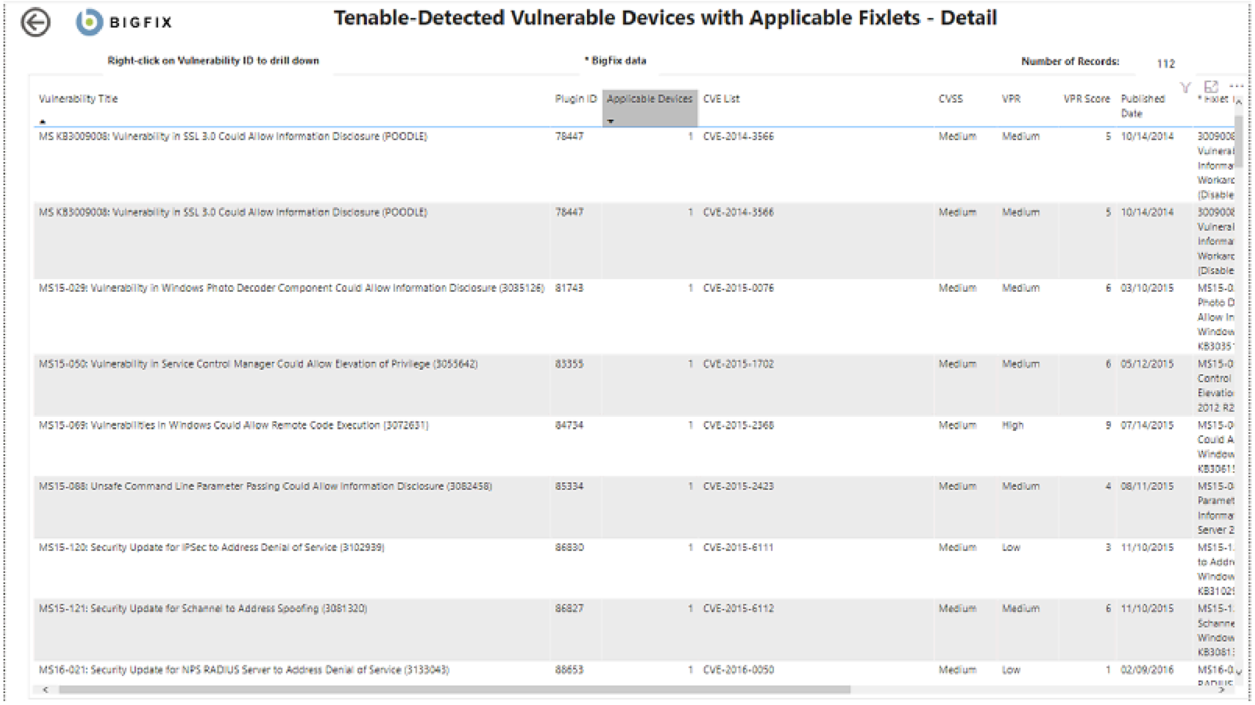
Chart details:

- Vulnerability Title - Vulnerability title
- PluginID - a unique identifier assigned to a vulnerability detection

- Applicable Devices - devices that have been scanned by Tenable and for which vulnerabilities have been identified
- CVE List - list of CVE
- CVSS2 - (Common Vulnerability Scoring System version 2), scoring system used to assess the severity and potential impact of security vulnerabilities.
- CVSS3 - (Common Vulnerability Scoring System version 3), updated version of the scoring system
- VPR - Vulnerability Priority Rating
- VPR Score - numerical value ranging from 0 to 10, with 10 being the highest priority
- Detected Date - the date when a vulnerability was first detected
- Published Date - date when the information about a vulnerability was first available
- ACR - Asset Criticality Rating: 1-10 rating that represents the asset's relative criticality based on device type, device purpose, and network location/proximity to the Internet.
- AES - Asset Exposure Score: A metric that combines ACR & VPR (Vulnerability Priority Rating) into a single score to represent an asset's relative exposure.

Detected Vulnerabilities with Applicable Fixlets





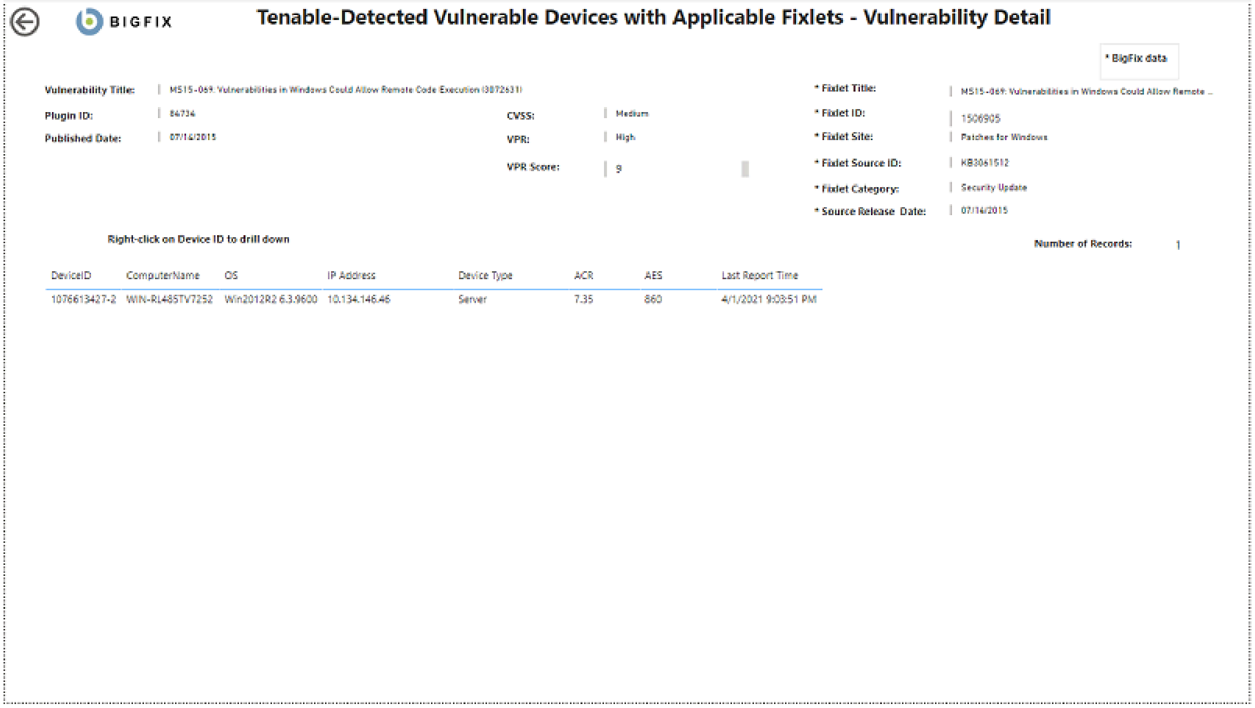
Tenable-Detected Vulnerable Devices with Applicable Fixlets - Detail

Right-click on Vulnerability ID to drill down

* BigFix data

Number of Records: 112

Vulnerability Title	Plugin ID	Applicable Devices	CVE List	CVSS	VPR	VPR Score	Published Date	* Fixlet I
MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	78447	1	CVE-2014-3566	Medium	Medium	5	10/14/2014	3009008 Vulnerat Informa Workarc (Disable
MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	78447	1	CVE-2014-3566	Medium	Medium	5	10/14/2014	3009008 Vulnerat Informa Workarc (Disable
MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure (3035126)	81743	1	CVE-2015-0076	Medium	Medium	6	03/10/2015	MS15-0. Photo D Allow In Window KB30351
MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege (3055642)	83355	1	CVE-2015-1702	Medium	Medium	6	05/12/2015	MS15-0 Control Elevatio 2012 R2
MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution (3072631)	84734	1	CVE-2015-2368	Medium	High	9	07/14/2015	MS15-0 Could A Window KB30615
MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure (3082458)	85334	1	CVE-2015-2423	Medium	Medium	4	08/11/2015	MS15-0 Paramet Informa Server 2
MS15-120: Security Update for IPSec to Address Denial of Service (3102939)	86830	1	CVE-2015-6111	Medium	Low	3	11/10/2015	MS15-1. to Addr Window KB31029
MS15-121: Security Update for Schannel to Address Spoofing (3081320)	86827	1	CVE-2015-6112	Medium	Medium	6	11/10/2015	MS15-1. Schanne Window KB30813
MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service (3133043)	88653	1	CVE-2016-0050	Medium	Low	1	02/09/2016	MS16-0 RADIUS



Tenable-Detected Vulnerable Devices with Applicable Fixlets - Vulnerability Detail

* BigFix data

Vulnerability Title: MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution (3072631)

Plugin ID: 84734

Published Date: 07/14/2015

CVSS: Medium

VPR: High

VPR Score: 9

* Fixlet Title: MS15-069: Vulnerabilities in Windows Could Allow Remote ...

* Fixlet ID: 1506905

* Fixlet Site: Patches for Windows

* Fixlet Source ID: KB3061512

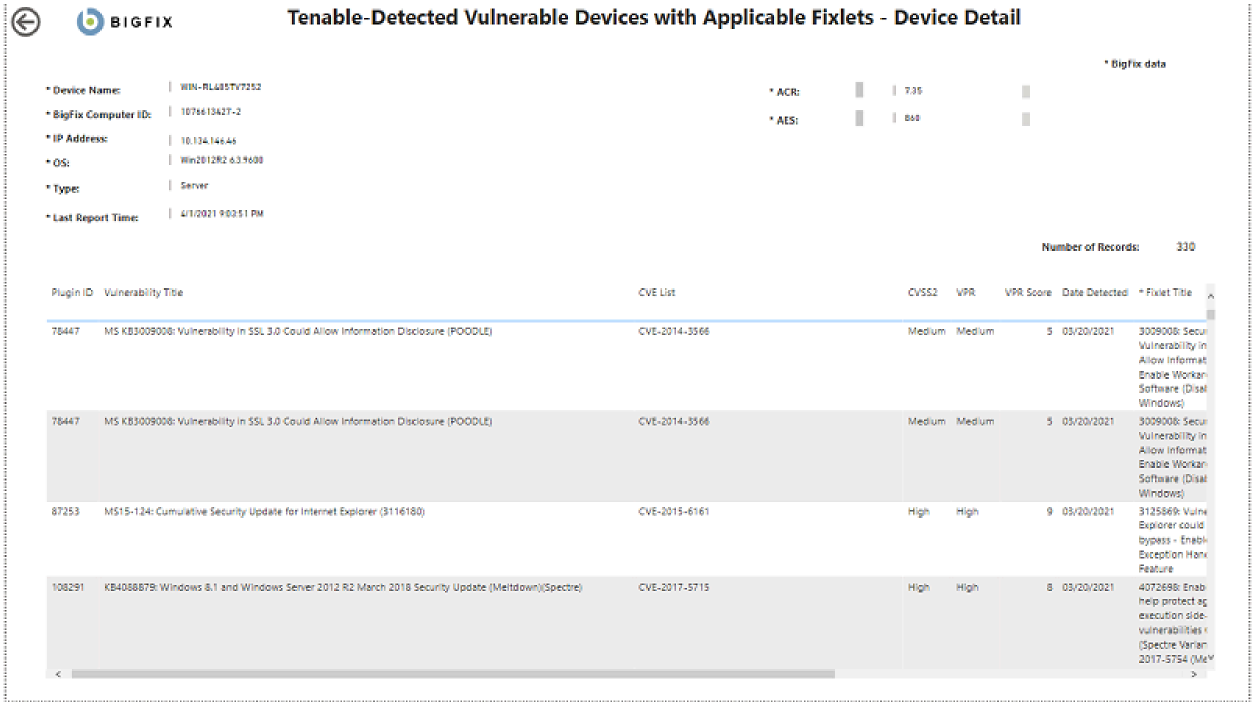
* Fixlet Category: Security Update

* Source Release Date: 07/14/2015

Right-click on Device ID to drill down

Number of Records: 1

DeviceID	ComputerName	OS	IP Address	Device Type	ACR	AES	Last Report Time
1076613427-2	WIN-RL485TV7252	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM



Tenable-Detected Vulnerable Devices with Applicable Fixlets - Device Detail

* BigFix data

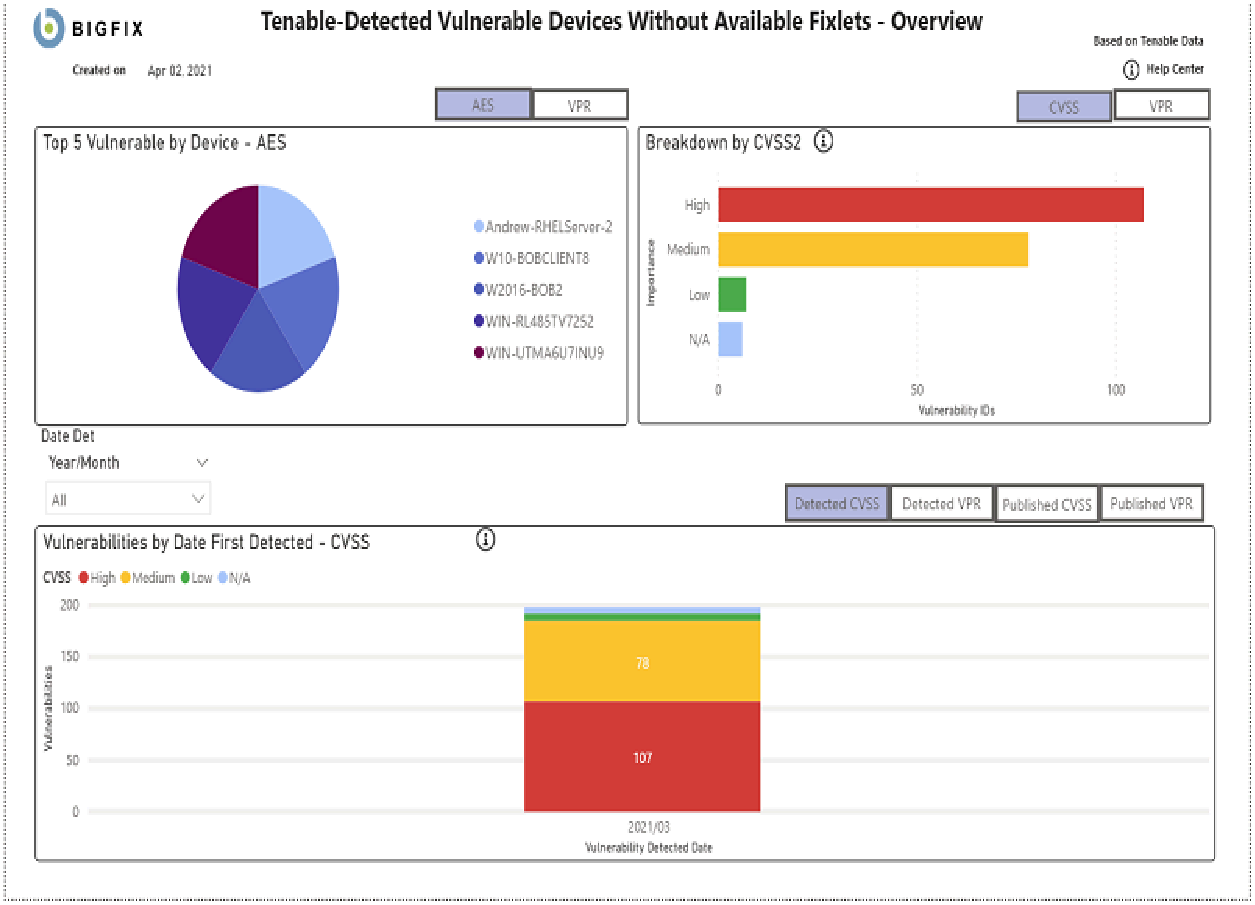
* Device Name:	WIN-RL485TV7252
* BigFix Computer ID:	1076613427-2
* IP Address:	10.134.146.46
* OS:	Win2012R2 6.3.9600
* Type:	Server
* Last Report Time:	4/1/2021 9:03:51 PM

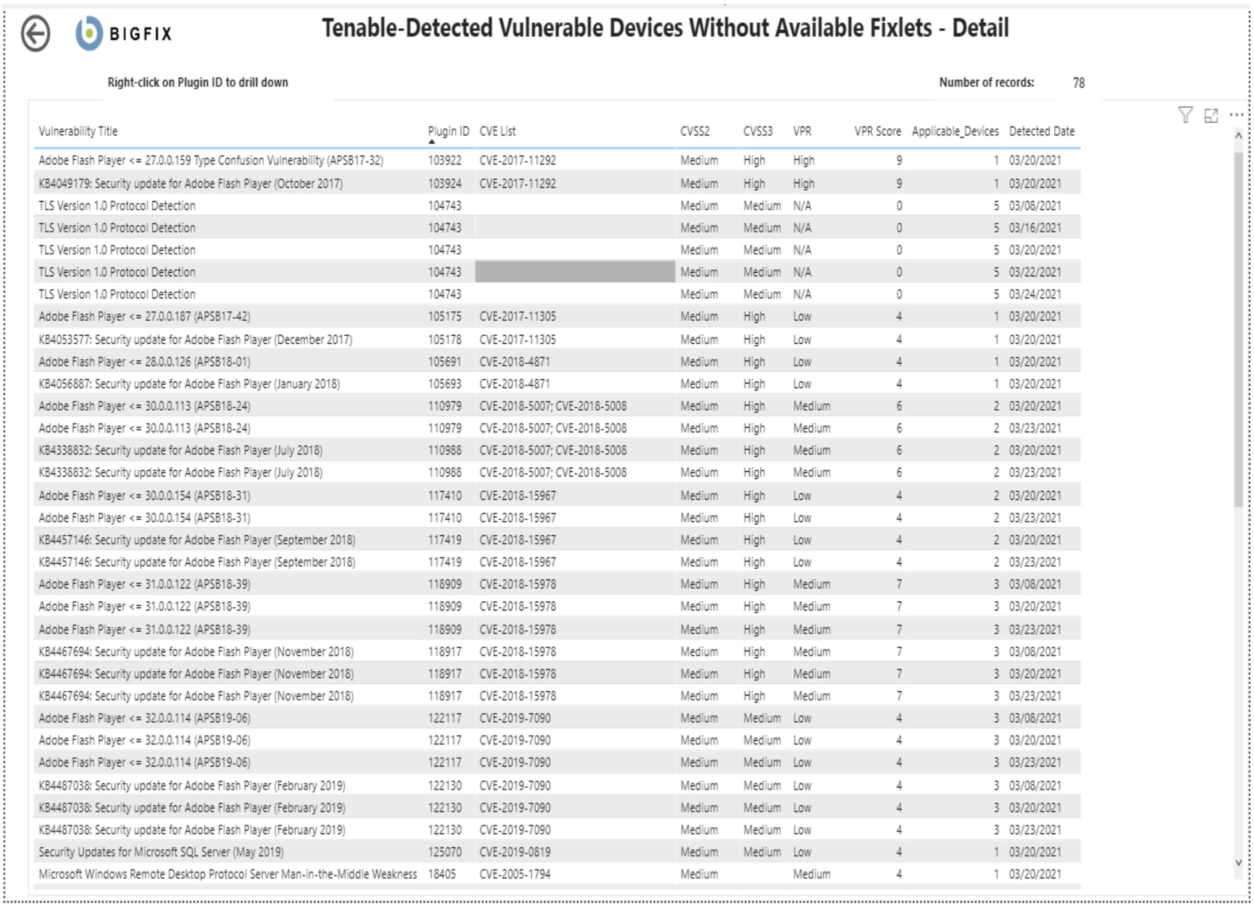
* ACR:	7.35
* AES:	868

Number of Records: 330

Plugin ID	Vulnerability Title	CVE List	CVSS2	VPR	VPR Score	Date Detected	* Fixlet Title
78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	CVE-2014-3566	Medium	Medium	5	03/20/2021	3009008: Secu Vulnerability in Allow Informat Enable Workar Software (Disal Windows)
78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	CVE-2014-3566	Medium	Medium	5	03/20/2021	3009008: Secu Vulnerability in Allow Informat Enable Workar Software (Disal Windows)
87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)	CVE-2015-6161	High	High	9	03/20/2021	3125869: Vulne Explorer could bypass - Enabl Exception Hanc Feature
108291	KB4088879: Windows 8.1 and Windows Server 2012 R2 March 2018 Security Update (Meltdown)(Spectre)	CVE-2017-5715	High	High	8	03/20/2021	4072698: Enab help protect ag execution side- vulnerabilities (Spectre Varian 2017-5754 (Me

Detected Vulnerabilities without Available Fixlets



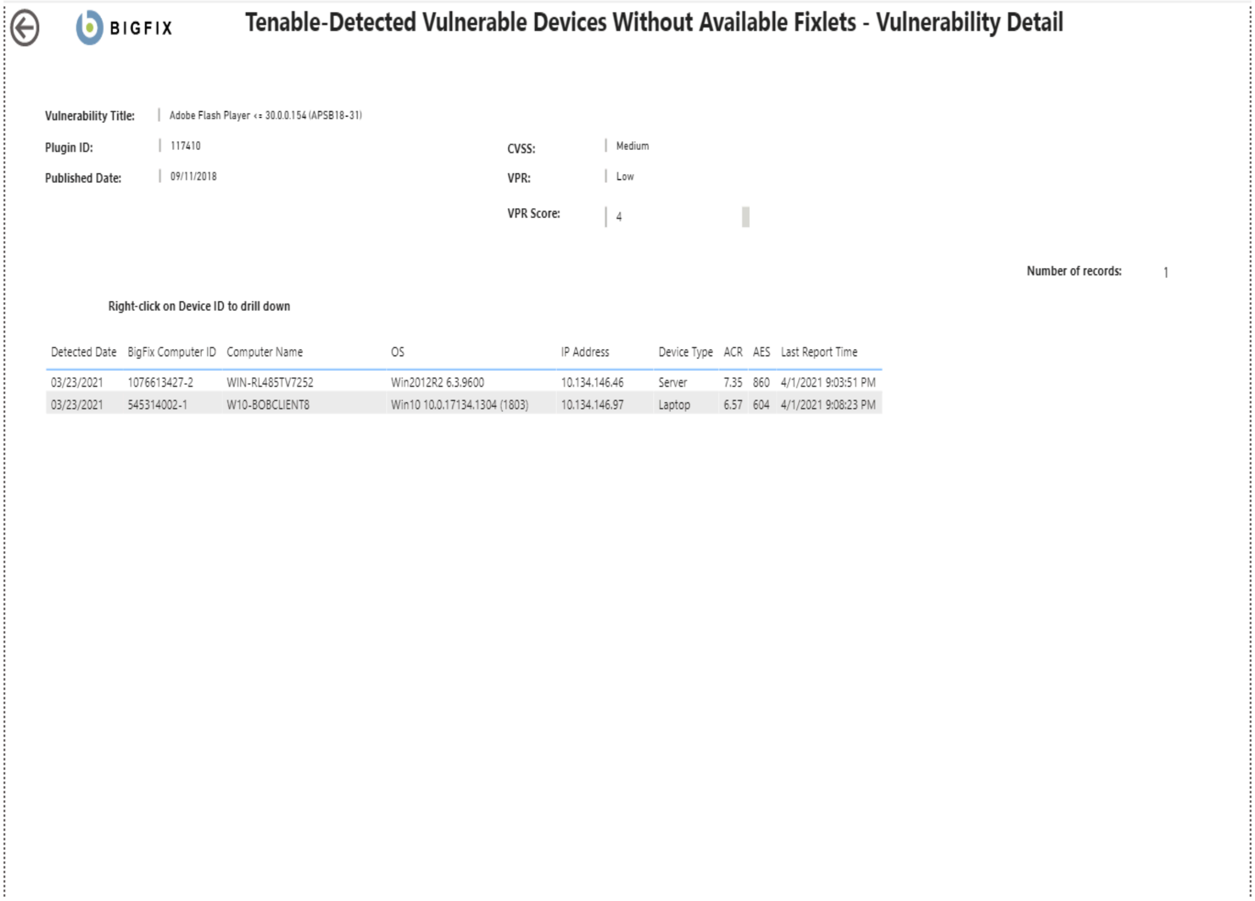


Tenable-Detected Vulnerable Devices Without Available Fixlets - Detail

Right-click on Plugin ID to drill down

Number of records: 78

Vulnerability Title	Plugin ID	CVE List	CVSS2	CVSS3	VPR	VPR Score	Applicable_Devices	Detected Date
Adobe Flash Player <= 27.0.0.159 Type Confusion Vulnerability (APSB17-32)	103922	CVE-2017-11292	Medium	High	High	9	1	03/20/2021
KB4049179: Security update for Adobe Flash Player (October 2017)	103924	CVE-2017-11292	Medium	High	High	9	1	03/20/2021
TLS Version 1.0 Protocol Detection	104743		Medium	Medium	N/A	0	5	03/08/2021
TLS Version 1.0 Protocol Detection	104743		Medium	Medium	N/A	0	5	03/16/2021
TLS Version 1.0 Protocol Detection	104743		Medium	Medium	N/A	0	5	03/20/2021
TLS Version 1.0 Protocol Detection	104743		Medium	Medium	N/A	0	5	03/22/2021
TLS Version 1.0 Protocol Detection	104743		Medium	Medium	N/A	0	5	03/24/2021
Adobe Flash Player <= 27.0.0.187 (APSB17-42)	105175	CVE-2017-11305	Medium	High	Low	4	1	03/20/2021
KB4053577: Security update for Adobe Flash Player (December 2017)	105178	CVE-2017-11305	Medium	High	Low	4	1	03/20/2021
Adobe Flash Player <= 28.0.0.126 (APSB18-01)	105691	CVE-2018-4871	Medium	High	Low	4	1	03/20/2021
KB4056887: Security update for Adobe Flash Player (January 2018)	105693	CVE-2018-4871	Medium	High	Low	4	1	03/20/2021
Adobe Flash Player <= 30.0.0.113 (APSB18-24)	110979	CVE-2018-5007; CVE-2018-5008	Medium	High	Medium	6	2	03/20/2021
Adobe Flash Player <= 30.0.0.113 (APSB18-24)	110979	CVE-2018-5007; CVE-2018-5008	Medium	High	Medium	6	2	03/23/2021
KB4338832: Security update for Adobe Flash Player (July 2018)	110988	CVE-2018-5007; CVE-2018-5008	Medium	High	Medium	6	2	03/20/2021
KB4338832: Security update for Adobe Flash Player (July 2018)	110988	CVE-2018-5007; CVE-2018-5008	Medium	High	Medium	6	2	03/23/2021
Adobe Flash Player <= 30.0.0.154 (APSB18-31)	117410	CVE-2018-15967	Medium	High	Low	4	2	03/20/2021
Adobe Flash Player <= 30.0.0.154 (APSB18-31)	117410	CVE-2018-15967	Medium	High	Low	4	2	03/23/2021
KB4457146: Security update for Adobe Flash Player (September 2018)	117419	CVE-2018-15967	Medium	High	Low	4	2	03/20/2021
KB4457146: Security update for Adobe Flash Player (September 2018)	117419	CVE-2018-15967	Medium	High	Low	4	2	03/23/2021
Adobe Flash Player <= 31.0.0.122 (APSB18-39)	118909	CVE-2018-15978	Medium	High	Medium	7	3	03/08/2021
Adobe Flash Player <= 31.0.0.122 (APSB18-39)	118909	CVE-2018-15978	Medium	High	Medium	7	3	03/20/2021
Adobe Flash Player <= 31.0.0.122 (APSB18-39)	118909	CVE-2018-15978	Medium	High	Medium	7	3	03/23/2021
KB4467694: Security update for Adobe Flash Player (November 2018)	118917	CVE-2018-15978	Medium	High	Medium	7	3	03/08/2021
KB4467694: Security update for Adobe Flash Player (November 2018)	118917	CVE-2018-15978	Medium	High	Medium	7	3	03/20/2021
KB4467694: Security update for Adobe Flash Player (November 2018)	118917	CVE-2018-15978	Medium	High	Medium	7	3	03/23/2021
Adobe Flash Player <= 32.0.0.114 (APSB19-06)	122117	CVE-2019-7090	Medium	Medium	Low	4	3	03/08/2021
Adobe Flash Player <= 32.0.0.114 (APSB19-06)	122117	CVE-2019-7090	Medium	Medium	Low	4	3	03/20/2021
Adobe Flash Player <= 32.0.0.114 (APSB19-06)	122117	CVE-2019-7090	Medium	Medium	Low	4	3	03/23/2021
KB4487038: Security update for Adobe Flash Player (February 2019)	122130	CVE-2019-7090	Medium	Medium	Low	4	3	03/08/2021
KB4487038: Security update for Adobe Flash Player (February 2019)	122130	CVE-2019-7090	Medium	Medium	Low	4	3	03/20/2021
KB4487038: Security update for Adobe Flash Player (February 2019)	122130	CVE-2019-7090	Medium	Medium	Low	4	3	03/23/2021
Security Updates for Microsoft SQL Server (May 2019)	125070	CVE-2019-0819	Medium	Medium	Low	4	1	03/20/2021
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	18405	CVE-2005-1794	Medium		Medium	4	1	03/20/2021



Tenable-Detected Vulnerable Devices Without Available Fixlets - Vulnerability Detail

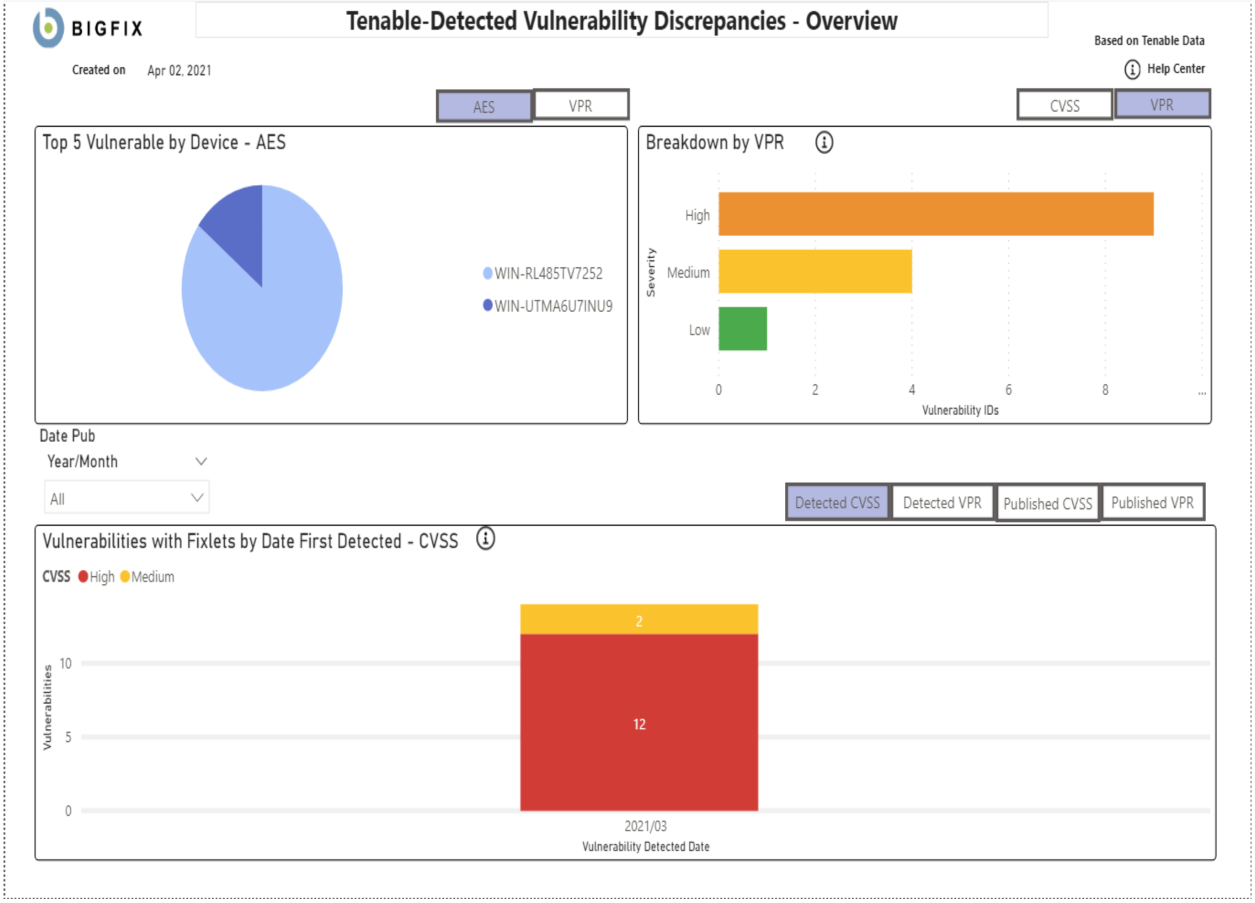
Vulnerability Title:	Adobe Flash Player <= 30.0.0.154 (APSB18-31)		
Plugin ID:	117410	CVSS:	Medium
Published Date:	09/11/2018	VPR:	Low
		VPR Score:	4

Number of records: 1

Right-click on Device ID to drill down

Detected Date	BigFix Computer ID	Computer Name	OS	IP Address	Device Type	ACR	AES	Last Report Time
03/23/2021	1076613427-2	WIN-RL485TV7252	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM
03/23/2021	545314002-1	W10-BOBCLIENT8	Win10 10.0.17134.1304 (1803)	10.134.146.97	Laptop	6.57	604	4/1/2021 9:08:23 PM

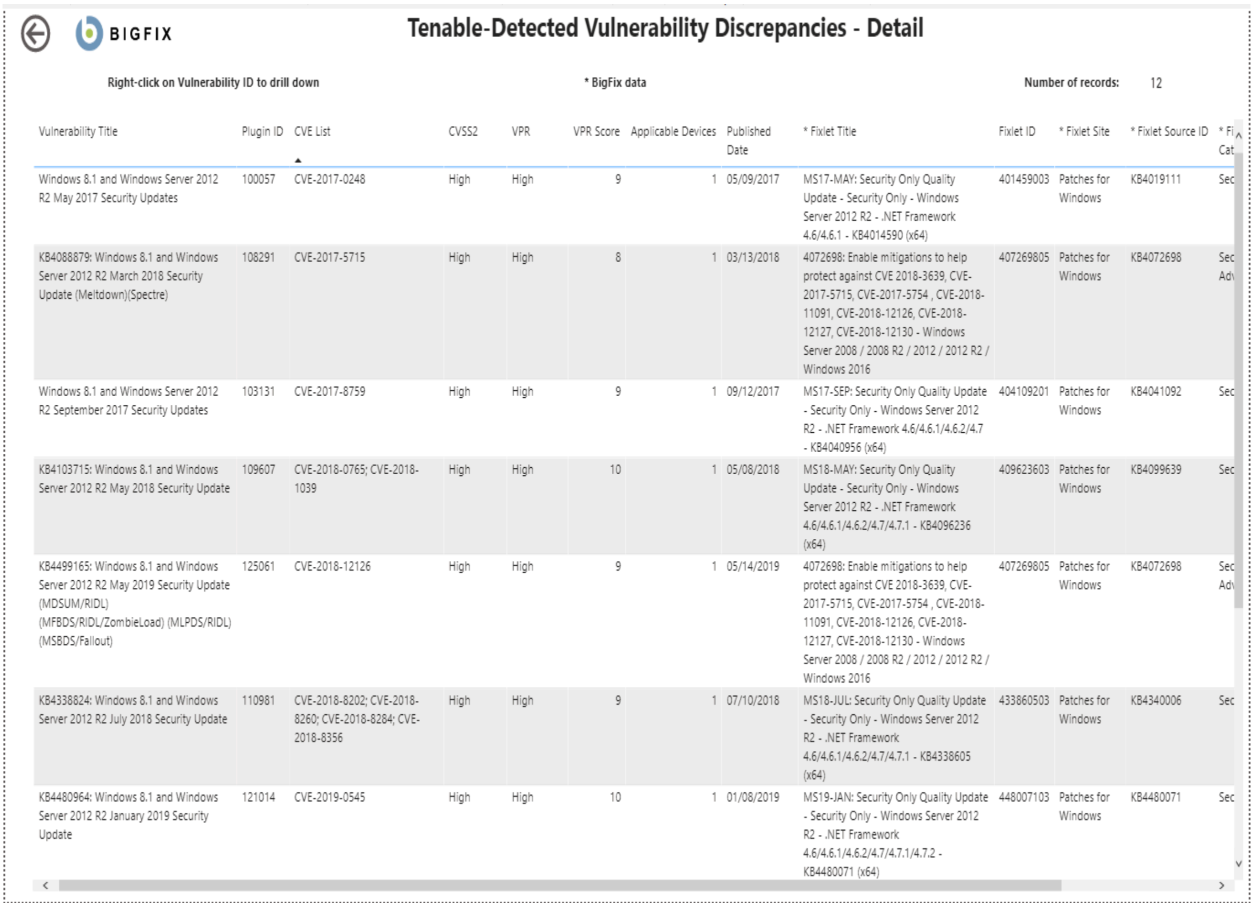
Vulnerability Discrepancies



Tenable-Detected Vulnerability Discrepancies - Overview

Created on Apr 02, 2021

Based on Tenable Data



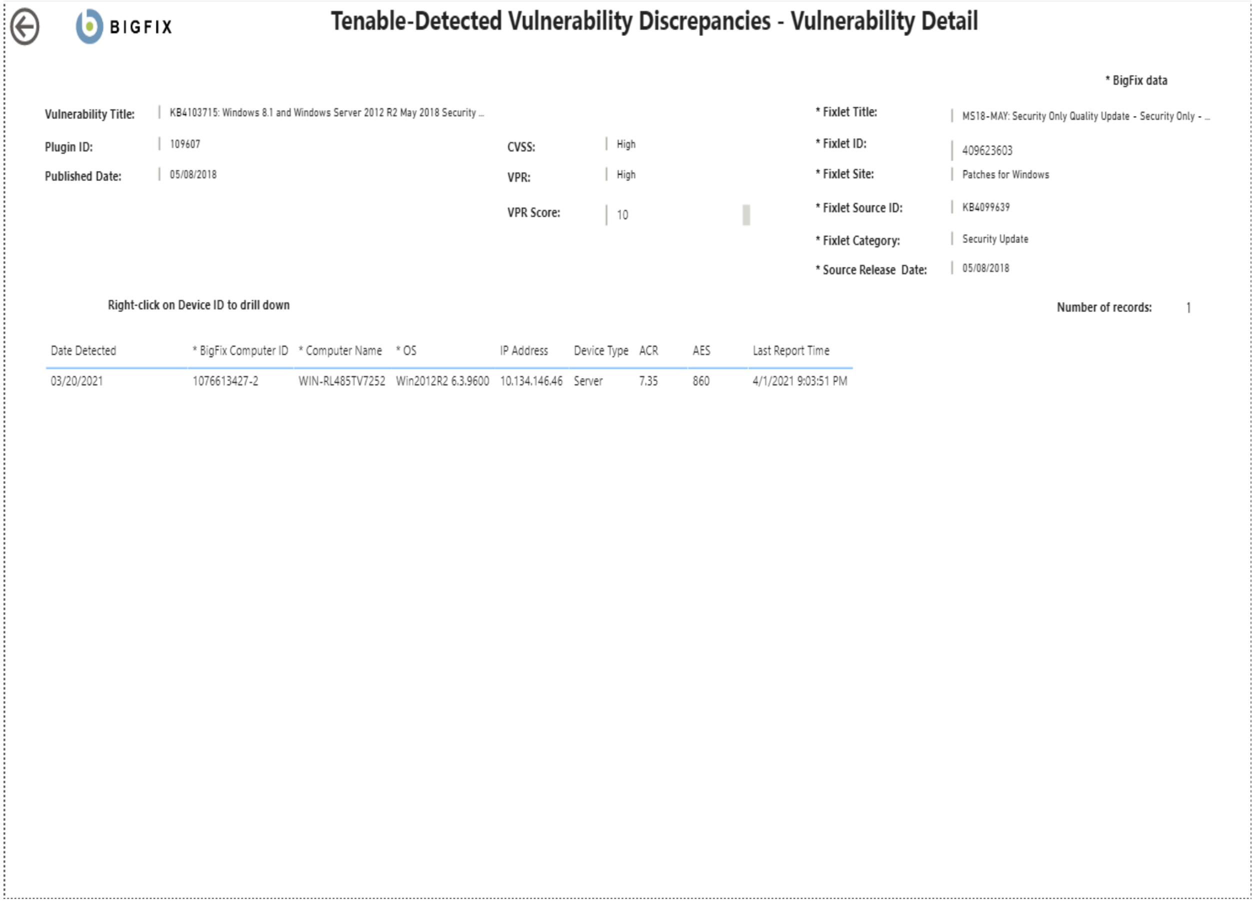
Tenable-Detected Vulnerability Discrepancies - Detail

Right-click on Vulnerability ID to drill down

* BigFix data

Number of records: 12

Vulnerability Title	Plugin ID	CVE List	CVSS2	VPR	VPR Score	Applicable Devices	Published Date	* Fixlet Title	Fixlet ID	* Fixlet Site	* Fixlet Source ID	* Fi Cat
Windows 8.1 and Windows Server 2012 R2 May 2017 Security Updates	100057	CVE-2017-0248	High	High	9	1	05/09/2017	MS17-MAY: Security Only Quality Update - Security Only - Windows Server 2012 R2 - .NET Framework 4.6/4.6.1 - KB4014590 (x64)	401459003	Patches for Windows	KB4019111	Sec
KB4088879: Windows 8.1 and Windows Server 2012 R2 March 2018 Security Update (Meltdown)(Spectre)	108291	CVE-2017-5715	High	High	8	1	03/13/2018	4072698: Enable mitigations to help protect against CVE 2018-3639, CVE-2017-5715, CVE-2017-5754 , CVE-2018-11091, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130 - Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / Windows 2016	407269805	Patches for Windows	KB4072698	Sec Adv
Windows 8.1 and Windows Server 2012 R2 September 2017 Security Updates	103131	CVE-2017-8759	High	High	9	1	09/12/2017	MS17-SEP: Security Only Quality Update - Security Only - Windows Server 2012 R2 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4040956 (x64)	404109201	Patches for Windows	KB4041092	Sec
KB4103715: Windows 8.1 and Windows Server 2012 R2 May 2018 Security Update	109607	CVE-2018-0765; CVE-2018-1039	High	High	10	1	05/08/2018	MS18-MAY: Security Only Quality Update - Security Only - Windows Server 2012 R2 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4096236 (x64)	409623603	Patches for Windows	KB4099639	Sec
KB4499165: Windows 8.1 and Windows Server 2012 R2 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)	125061	CVE-2018-12126	High	High	9	1	05/14/2019	4072698: Enable mitigations to help protect against CVE 2018-3639, CVE-2017-5715, CVE-2017-5754 , CVE-2018-11091, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130 - Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / Windows 2016	407269805	Patches for Windows	KB4072698	Sec Adv
KB4338824: Windows 8.1 and Windows Server 2012 R2 July 2018 Security Update	110981	CVE-2018-8202; CVE-2018-8260; CVE-2018-8284; CVE-2018-8356	High	High	9	1	07/10/2018	MS18-JUL: Security Only Quality Update - Security Only - Windows Server 2012 R2 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4338605 (x64)	433860503	Patches for Windows	KB4340006	Sec
KB4480964: Windows 8.1 and Windows Server 2012 R2 January 2019 Security Update	121014	CVE-2019-0545	High	High	10	1	01/08/2019	MS19-JAN: Security Only Quality Update - Security Only - Windows Server 2012 R2 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4480071 (x64)	448007103	Patches for Windows	KB4480071	Sec



Tenable-Detected Vulnerability Discrepancies - Vulnerability Detail

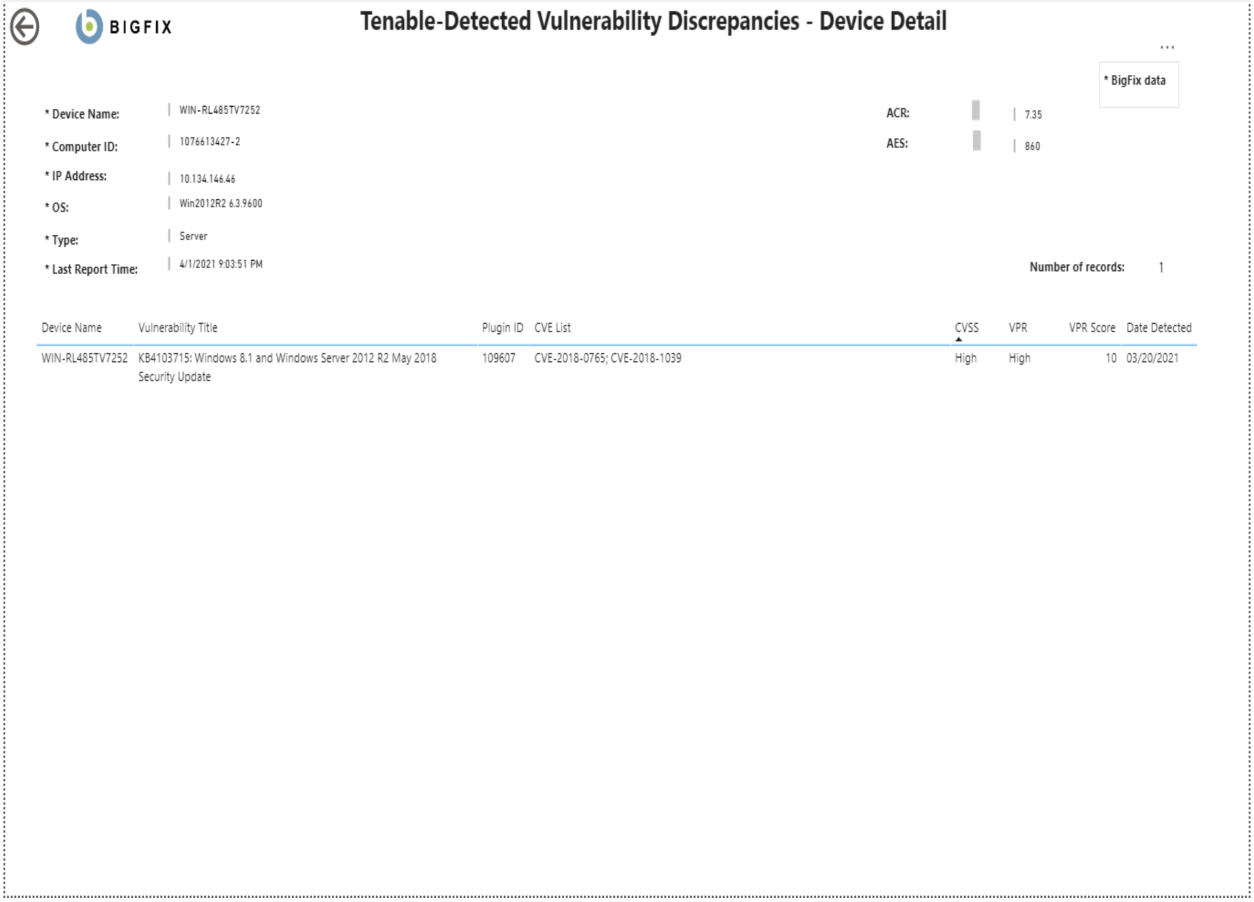
* BigFix data

Vulnerability Title:	KB4103715: Windows 8.1 and Windows Server 2012 R2 May 2018 Security ...
Plugin ID:	109607
Published Date:	05/08/2018
CVSS:	High
VPR:	High
VPR Score:	10
* Fixlet Title:	MS18-MAY: Security Only Quality Update - Security Only - ...
* Fixlet ID:	409623603
* Fixlet Site:	Patches for Windows
* Fixlet Source ID:	KB4099639
* Fixlet Category:	Security Update
* Source Release Date:	05/08/2018

Right-click on Device ID to drill down

Number of records: 1

Date Detected	* BigFix Computer ID	* Computer Name	* OS	IP Address	Device Type	ACR	AES	Last Report Time
03/20/2021	1076613427-2	WIN-RL485TV7252	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM



Tenable-Detected Vulnerability Discrepancies - Device Detail

* BigFix data

* Device Name:	WIN-RL485TV7252	ACR:	7.35
* Computer ID:	1076613427-2	AES:	860
* IP Address:	10.134.146.46		
* OS:	Win2012R2 6.3.9600		
* Type:	Server		
* Last Report Time:	4/1/2021 9:03:51 PM	Number of records:	1

Device Name	Vulnerability Title	Plugin ID	CVE List	CVSS	VPR	VPR Score	Date Detected
WIN-RL485TV7252	KB4103715: Windows 8.1 and Windows Server 2012 R2 May 2018 Security Update	109607	CVE-2018-0765; CVE-2018-1039	High	High	10	03/20/2021

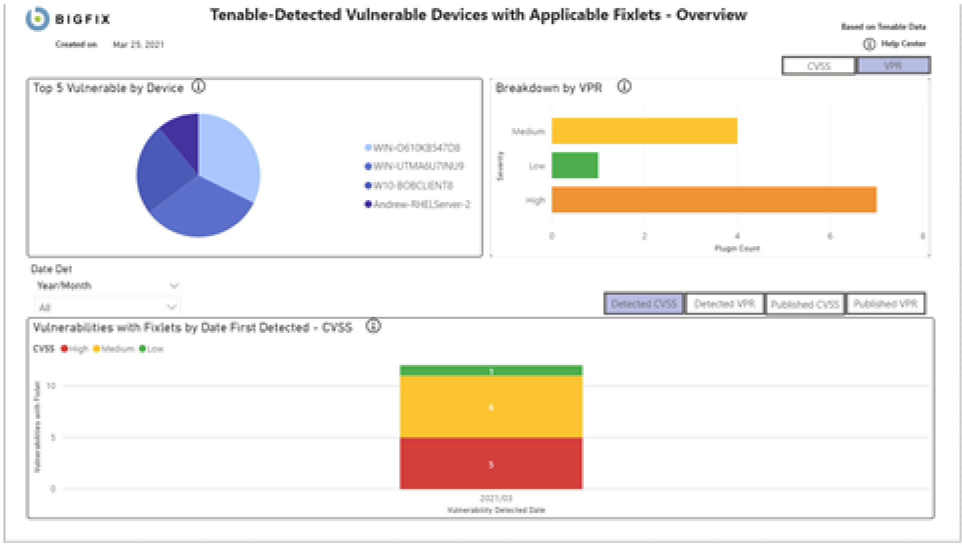
Power BI reports for Tenable.sc

Use this section to become familiar with Power BI reports for Tenable.sc.

Chart details:

- Vulnerability Title - Vulnerability title
- PluginID - a unique identifier assigned to a vulnerability detection
- Applicable Devices - devices that have been scanned by Tenable and for which vulnerabilities have been identified
- CVE List - list of CVE
- CVSS2 - (Common Vulnerability Scoring System version 2), scoring system used to assess the severity and potential impact of security vulnerabilities.
- CVSS3 - (Common Vulnerability Scoring System version 3), updated version of the scoring system
- VPR - Vulnerability Priority Rating
- VPR Score - numerical value ranging from 0 to 10, with 10 being the highest priority
- Detected Date - the date when a vulnerability was first detected
- Published Date - date when the information about a vulnerability was first available

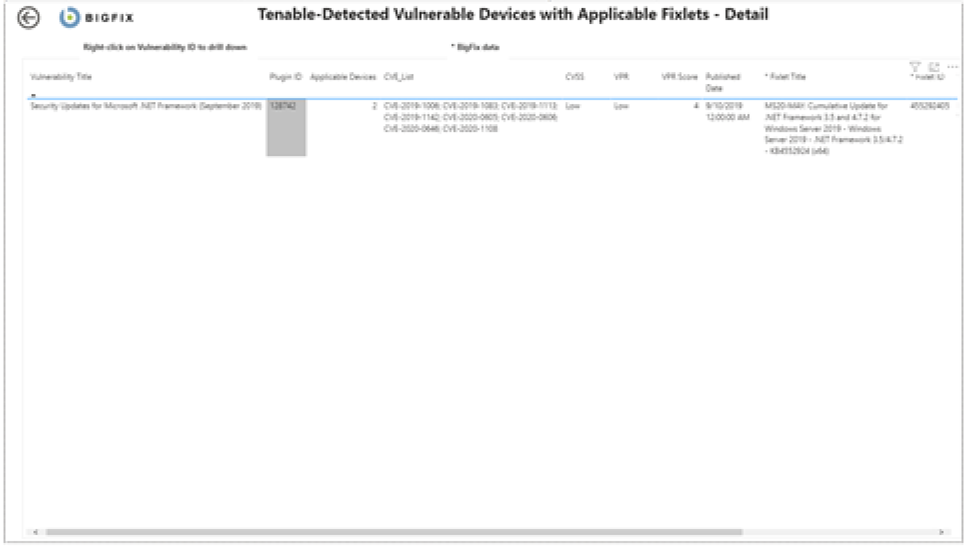
Detected Vulnerabilities with Applicable Fixlets



Tenable-Detected Vulnerable Devices with Applicable Fixlets - Overview

Created on Mar 25, 2021

Based on Tenable Data

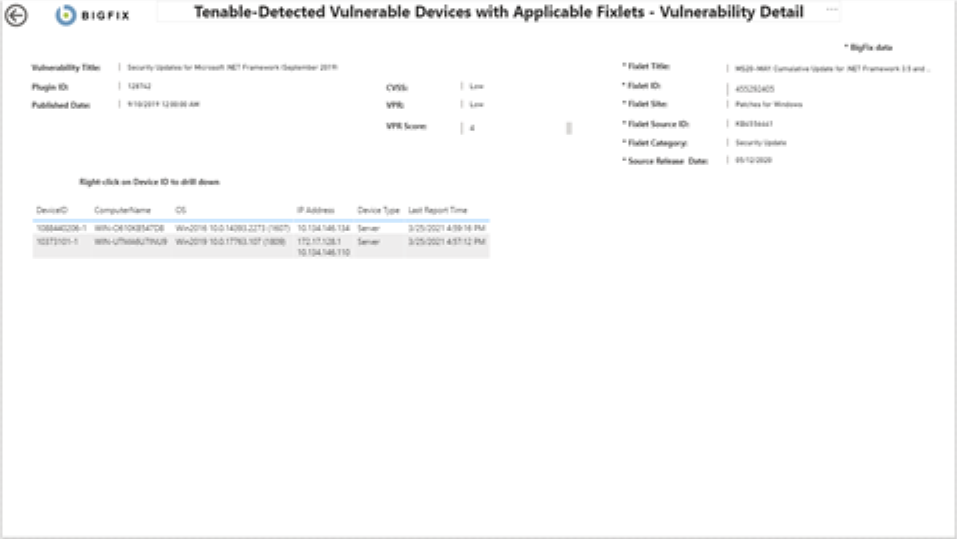


Tenable-Detected Vulnerable Devices with Applicable Fixlets - Detail

Right-click on Vulnerability ID to drill down

* BigFix data

Vulnerability Title	Plugin ID	Applicable Devices	CVE_List	CVSS	VPR	VPR Score	Published Date	* Fixlet Title	* Fixlet ID
Security Updates for Microsoft .NET Framework (September 2019)	128742	2	CVE-2019-1006; CVE-2019-1083; CVE-2019-1113; CVE-2019-1142; CVE-2020-0605; CVE-2020-0606; CVE-2020-0646; CVE-2020-1108	Low	Low	4	9/10/2019 12:00:00 AM	MS20-MAY: Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 - Windows Server 2019 - .NET Framework 3.5/4.7.2 - KB4552924 (x64)	455292405



Tenable-Detected Vulnerable Devices with Applicable Fixlets - Vulnerability Detail

* BigFix data

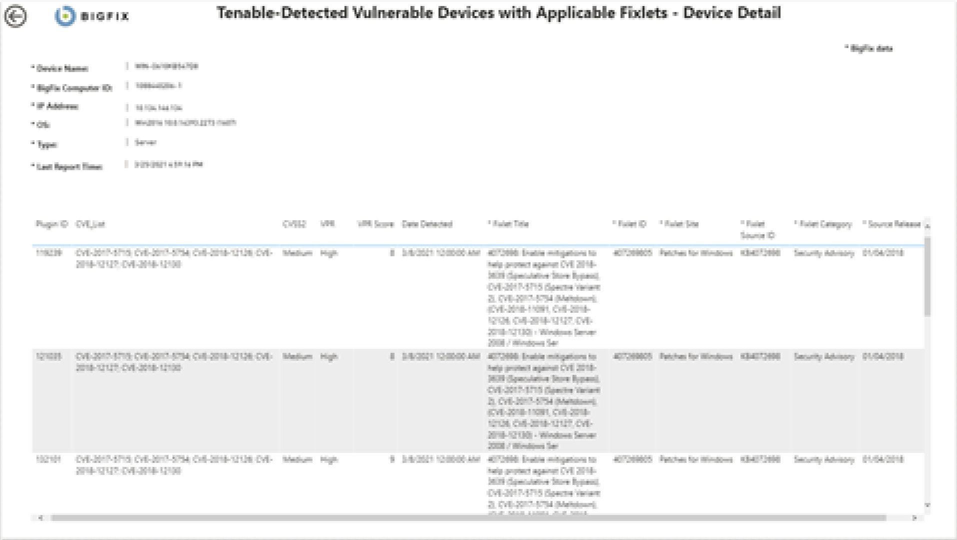
Vulnerability Title: Security Updates for Microsoft .NET Framework (September 2019)
Plugin ID: 128742
Published Date: 9/10/2019 12:00:00 AM

CVSS: Low
VPR: Low
VPR Score: 4

* Fixlet Title: MS20-MAY: Cumulative Update for .NET Framework 3.5 and ...
* Fixlet ID: 455292405
* Fixlet Site: Patches for Windows
* Fixlet Source ID: KB4556441
* Fixlet Category: Security Update
* Source Release Date: 05/12/2020

Right-click on Device ID to drill down

DeviceID	ComputerName	OS	IP Address	Device Type	Last Report Time
1088440206-1	WIN-O610KB547D8	Win2016 10.0.14393.2273 (1607)	10.134.146.134	Server	3/25/2021 4:59:16 PM
10373101-1	WIN-UTN66U7NU9	Win2019 10.0.17763.107 (1809)	172.17.128.1 10.134.146.110	Server	3/25/2021 4:57:12 PM



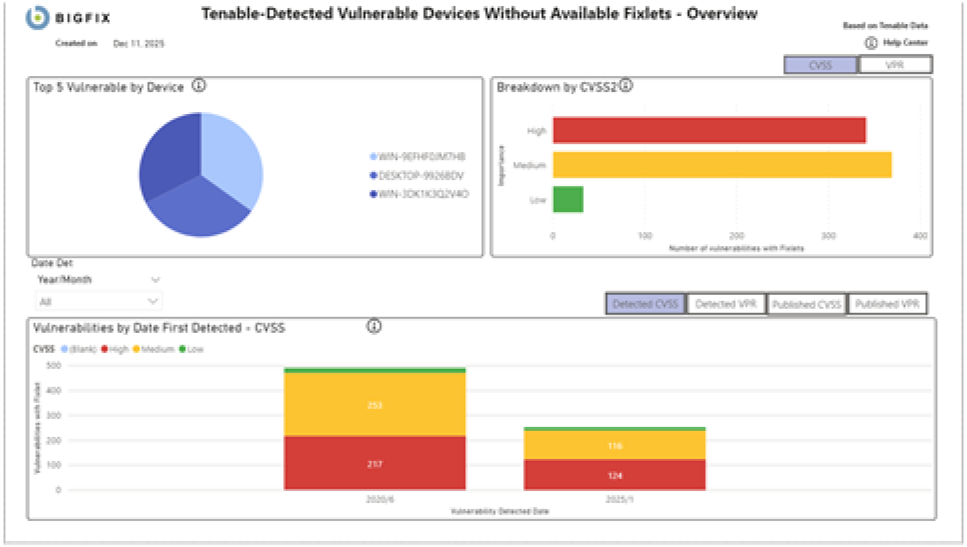
Tenable-Detected Vulnerable Devices with Applicable Fixlets - Device Detail

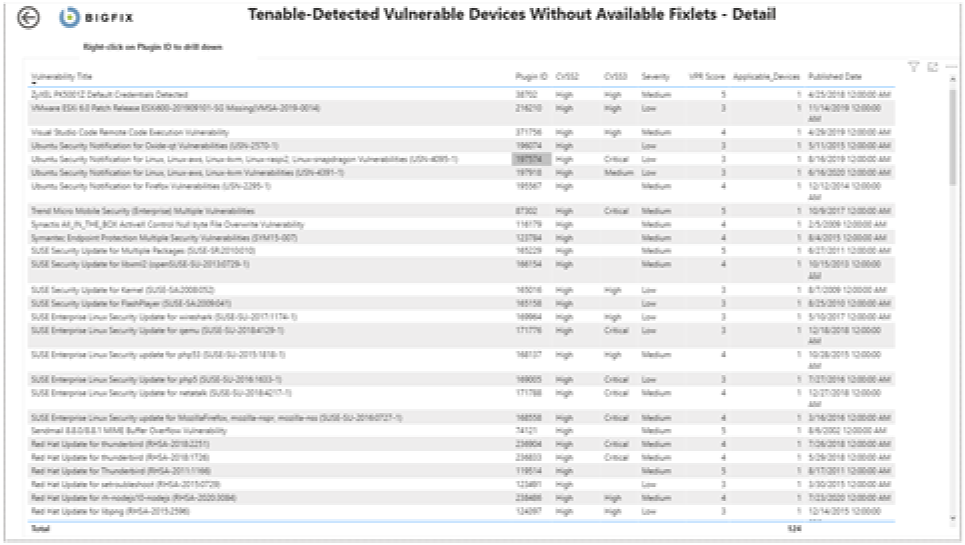
* BigFix data

* Device Name: WIN-O610KB547D8
* BigFix Computer ID: 1088440206-1
* IP Address: 10.134.146.134
* OS: Win2016 10.0.14393.2273 (1607)
* Type: Server
* Last Report Time: 3/25/2021 4:59:16 PM

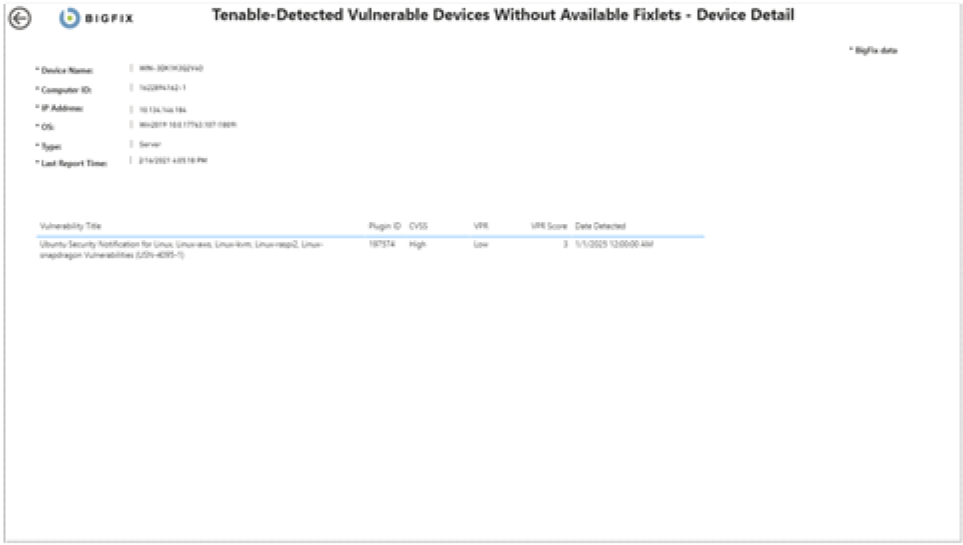
Plugin ID	CVE_List	CVSS2	VPR	VPR Score	Date Detected	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Source ID	* Fixlet Category	* Source Release
119239	CVE-2017-5715; CVE-2017-5754; CVE-2018-12126; CVE-2018-12127; CVE-2018-12130	Medium	High	8	3/8/2021 12:00:00 AM	4072698: Enable mitigations to help protect against CVE 2018-3639 (Speculative Store Bypass), CVE-2017-5715 (Spectre Variant 2), CVE-2017-5754 (Meltdown), (CVE-2018-11091, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130) - Windows Server 2008 / Windows Ser	407269805	Patches for Windows	KB4072698	Security Advisory	01/04/2018
121035	CVE-2017-5715; CVE-2017-5754; CVE-2018-12126; CVE-2018-12127; CVE-2018-12130	Medium	High	8	3/8/2021 12:00:00 AM	4072698: Enable mitigations to help protect against CVE 2018-3639 (Speculative Store Bypass), CVE-2017-5715 (Spectre Variant 2), CVE-2017-5754 (Meltdown), (CVE-2018-11091, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130) - Windows Server 2008 / Windows Ser	407269805	Patches for Windows	KB4072698	Security Advisory	01/04/2018
132101	CVE-2017-5715; CVE-2017-5754; CVE-2018-12126; CVE-2018-12127; CVE-2018-12130	Medium	High	9	3/8/2021 12:00:00 AM	4072698: Enable mitigations to help protect against CVE 2018-3639 (Speculative Store Bypass), CVE-2017-5715 (Spectre Variant 2), CVE-2017-5754 (Meltdown),	407269805	Patches for Windows	KB4072698	Security Advisory	01/04/2018

Detected Vulnerabilities without Available Fixlets




BIGFIX
Tenable-Detected Vulnerable Devices Without Available Fixlets - Detail
Right-click on Plugin ID to drill down

Vulnerability Title	Plugin ID	CVSS2	CVSS3	Severity	VPR Score	Applicable_Devices	Published Date
ZyXEL PK5001Z Default Credentials Detected	38702	High	High	Medium	5	1	4/25/2018 12:00:00 AM
VMware ESXi 6.0 Patch Release ESXi600-201909101-SG Missing(VMSA-2019-0014)	216210	High	High	Low	3	1	11/14/2019 12:00:00 AM
Visual Studio Code Remote Code Execution Vulnerability	371756	High	High	Medium	4	1	4/29/2019 12:00:00 AM
Ubuntu Security Notification for Oxide-qt Vulnerabilities (USN-2570-1)	196074	High		Low	3	1	5/11/2015 12:00:00 AM
Ubuntu Security Notification for Linux, Linux-aws, Linux-kvm, Linux-raspi2, Linux-snapdragon Vulnerabilities (USN-4095-1)	197574	High	Critical	Low	3	1	8/16/2019 12:00:00 AM
Ubuntu Security Notification for Linux, Linux-aws, Linux-kvm Vulnerabilities (USN-4391-1)	197918	High	Medium	Low	3	1	6/16/2020 12:00:00 AM
Ubuntu Security Notification for Firefox Vulnerabilities (USN-2295-1)	195567	High		Medium	4	1	12/12/2014 12:00:00 AM
Trend Micro Mobile Security (Enterprise) Multiple Vulnerabilities	87302	High	Critical	Medium	5	1	10/9/2017 12:00:00 AM
Synactis All_IN_THE_BOX ActiveX Control Null-byte File Overwrite Vulnerability	116179	High		Medium	4	1	2/5/2009 12:00:00 AM
Symantec Endpoint Protection Multiple Security Vulnerabilities (SYM15-007)	123784	High		Medium	4	1	8/4/2015 12:00:00 AM
SUSE Security Update for Multiple Packages (SUSE-SR:2010:010)	165229	High		Medium	5	1	6/27/2011 12:00:00 AM
SUSE Security Update for libxml2 (openSUSE-SU-2013:0729-1)	166154	High		Medium	4	1	10/15/2013 12:00:00 AM
SUSE Security Update for Kernel (SUSE-SA:2008:052)	165016	High	High	Low	3	1	8/7/2009 12:00:00 AM
SUSE Security Update for FlashPlayer (SUSE-SA:2009:041)	165158	High		Low	3	1	8/25/2010 12:00:00 AM
SUSE Enterprise Linux Security Update for wireshark (SUSE-SU-2017:1174-1)	169964	High	High	Low	3	1	5/10/2017 12:00:00 AM
SUSE Enterprise Linux Security Update for qemu (SUSE-SU-2018:4129-1)	171776	High	Critical	Low	3	1	12/18/2018 12:00:00 AM
SUSE Enterprise Linux Security update for php53 (SUSE-SU-2015:1818-1)	168137	High	High	Medium	4	1	10/28/2015 12:00:00 AM
SUSE Enterprise Linux Security Update for php5 (SUSE-SU-2016:1603-1)	169005	High	Critical	Low	3	1	7/27/2016 12:00:00 AM
SUSE Enterprise Linux Security Update for netatalk (SUSE-SU-2018:4217-1)	171788	High	Critical	Medium	4	1	12/27/2018 12:00:00 AM
SUSE Enterprise Linux Security update for MozillaFirefox, mozilla-nspr, mozilla-nss (SUSE-SU-2016:0727-1)	168558	High	Critical	Medium	4	1	3/16/2016 12:00:00 AM
Sendmail 8.8.0/8.8.1 MIME Buffer Overflow Vulnerability	74121	High		Medium	5	1	8/6/2002 12:00:00 AM
Red Hat Update for thunderbird (RHSA-2018:2251)	236904	High	Critical	Medium	4	1	7/26/2018 12:00:00 AM
Red Hat Update for thunderbird (RHSA-2018:1726)	236853	High	Critical	Medium	4	1	5/29/2018 12:00:00 AM
Red Hat Update for Thunderbird (RHSA-2011:1166)	119514	High		Medium	5	1	8/17/2011 12:00:00 AM
Red Hat Update for setroubleshoot (RHSA-2015:0729)	123491	High		Low	3	1	3/30/2015 12:00:00 AM
Red Hat Update for rh-nodejs10-nodejs (RHSA-2020:3084)	238486	High	High	Medium	4	1	7/23/2020 12:00:00 AM
Red Hat Update for libpng (RHSA-2015:2596)	124097	High	High	Low	3	1	12/14/2015 12:00:00
Total						124	



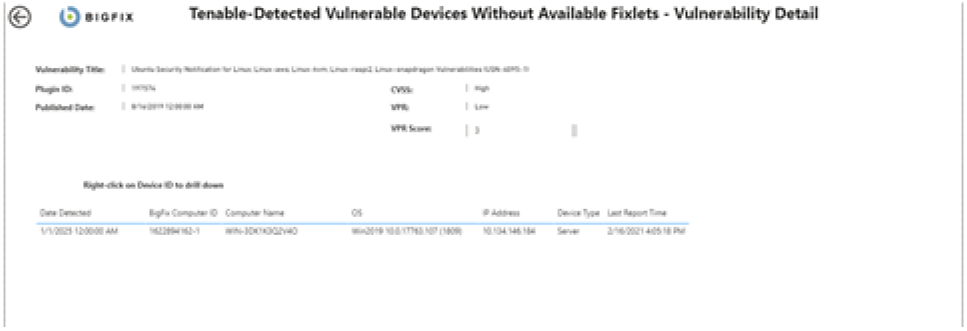
BIGFIX

Tenable-Detected Vulnerable Devices Without Available Fixlets - Device Detail

* BigFix data

* Device Name: | WIN-3DK1KDQ2V4O
* Computer ID: | 1622894162-1
* IP Address: | 10.134.146.184
* OS: | Win2019 10.0.17763.107 (1809)
* Type: | Server
* Last Report Time: | 2/16/2021 4:05:18 PM

Vulnerability Title	Plugin ID	CVSS	VPR	VPR Score	Date Detected
Ubuntu Security Notification for Linux, Linux-aws, Linux-kvm, Linux-raspi2, Linux-snapdragon Vulnerabilities (USN-4095-1)	197574	High	Low	3	1/1/2025 12:00:00 AM



BIGFIX

Tenable-Detected Vulnerable Devices Without Available Fixlets - Vulnerability Detail

Vulnerability Title: | Ubuntu Security Notification for Linux, Linux-aws, Linux-kvm, Linux-raspi2, Linux-snapdragon Vulnerabilities (USN-4095-1)

Plugin ID: | 197574

Published Date: | 8/14/2019 12:00:00 AM

CVSS: | High

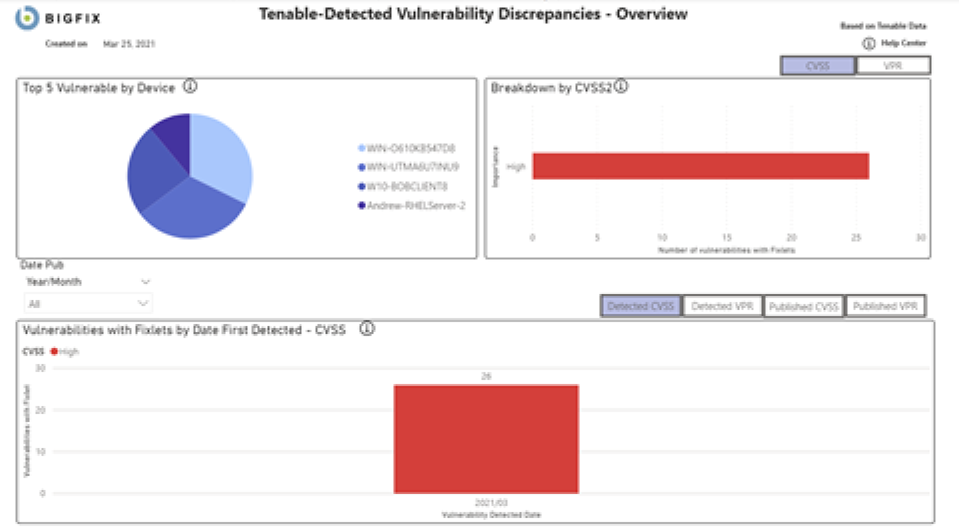
VPR: | Low

VPR Score: | 3

Right-click on Device ID to drill down

Date Detected	BigFix Computer ID	Computer Name	OS	IP Address	Device Type	Last Report Time
1/1/2025 12:00:00 AM	1622894162-1	WIN-3DK1KDQ2V4O	Win2019 10.0.17763.107 (1809)	10.134.146.184	Server	2/16/2021 4:05:18 PM

Vulnerability Discrepancies

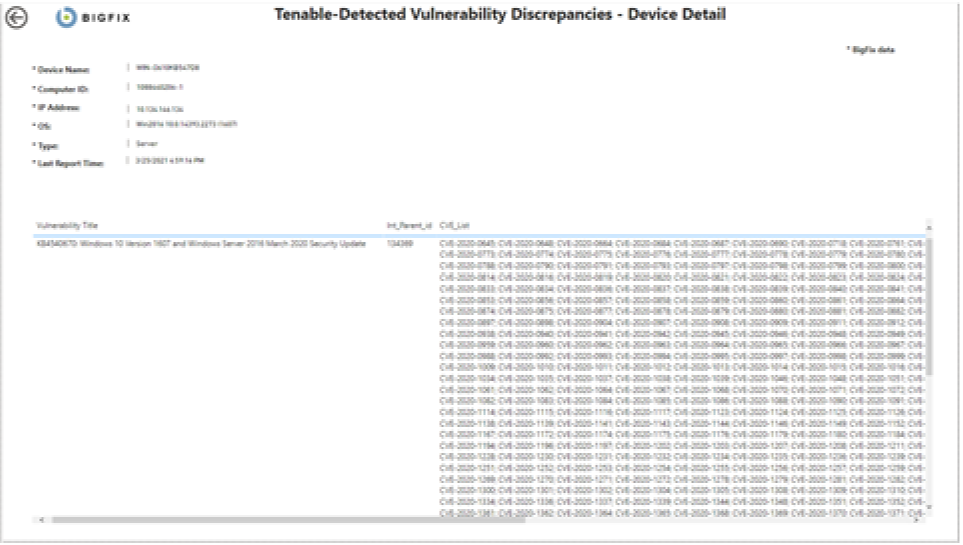


BIGFIX

Tenable-Detected Vulnerability Discrepancies - Overview

Created on Mar 25, 2021

Based on Tenable Data



Tenable-Detected Vulnerability Discrepancies - Device Detail

* BigFix data

* Device Name: WIN-C610KB547D8

* Computer ID: 1088640206-1

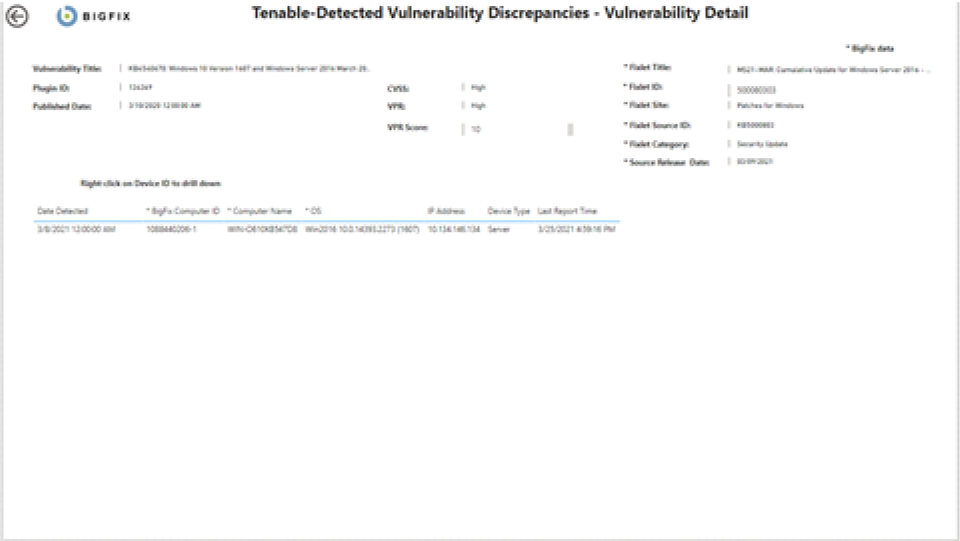
* IP Address: 10.134.146.134

* OS: Win2016 10.0.14393.2273 (1607)

* Type: Server

* Last Report Time: 3/25/2021 4:59:16 PM

Vulnerability Title	Int_Parent_id	CVE_List
KB4540670: Windows 10 Version 1607 and Windows Server 2016 March 2020 Security Update	134369	CVE-2020-0645; CVE-2020-0648; CVE-2020-0664; CVE-2020-0684; CVE-2020-0687; CVE-2020-0690; CVE-2020-0718; CVE-2020-0761; CVE-2020-0773; CVE-2020-0774; CVE-2020-0775; CVE-2020-0776; CVE-2020-0777; CVE-2020-0778; CVE-2020-0779; CVE-2020-0780; CVE-2020-0788; CVE-2020-0790; CVE-2020-0791; CVE-2020-0793; CVE-2020-0797; CVE-2020-0798; CVE-2020-0799; CVE-2020-0800; CVE-2020-0814; CVE-2020-0816; CVE-2020-0819; CVE-2020-0820; CVE-2020-0821; CVE-2020-0822; CVE-2020-0823; CVE-2020-0824; CVE-2020-0833; CVE-2020-0834; CVE-2020-0836; CVE-2020-0837; CVE-2020-0838; CVE-2020-0839; CVE-2020-0840; CVE-2020-0841; CVE-2020-0853; CVE-2020-0856; CVE-2020-0857; CVE-2020-0858; CVE-2020-0859; CVE-2020-0860; CVE-2020-0861; CVE-2020-0864; CVE-2020-0874; CVE-2020-0875; CVE-2020-0877; CVE-2020-0878; CVE-2020-0879; CVE-2020-0880; CVE-2020-0881; CVE-2020-0882; CVE-2020-0897; CVE-2020-0898; CVE-2020-0904; CVE-2020-0907; CVE-2020-0908; CVE-2020-0909; CVE-2020-0911; CVE-2020-0912; CVE-2020-0938; CVE-2020-0940; CVE-2020-0941; CVE-2020-0942; CVE-2020-0945; CVE-2020-0946; CVE-2020-0948; CVE-2020-0949; CVE-2020-0959; CVE-2020-0960; CVE-2020-0962; CVE-2020-0963; CVE-2020-0964; CVE-2020-0965; CVE-2020-0966; CVE-2020-0967; CVE-2020-0988; CVE-2020-0992; CVE-2020-0993; CVE-2020-0994; CVE-2020-0995; CVE-2020-0997; CVE-2020-0998; CVE-2020-0999; CVE-2020-1009; CVE-2020-1010; CVE-2020-1011; CVE-2020-1012; CVE-2020-1013; CVE-2020-1014; CVE-2020-1015; CVE-2020-1016; CVE-2020-1034; CVE-2020-1035; CVE-2020-1037; CVE-2020-1038; CVE-2020-1039; CVE-2020-1046; CVE-2020-1048; CVE-2020-1051; CVE-2020-1061; CVE-2020-1062; CVE-2020-1064; CVE-2020-1067; CVE-2020-1068; CVE-2020-1070; CVE-2020-1071; CVE-2020-1072; CVE-2020-1082; CVE-2020-1083; CVE-2020-1084; CVE-2020-1085; CVE-2020-1086; CVE-2020-1088; CVE-2020-1090; CVE-2020-1091; CVE-2020-1114; CVE-2020-1115; CVE-2020-1116; CVE-2020-1117; CVE-2020-1123; CVE-2020-1124; CVE-2020-1125; CVE-2020-1126; CVE-2020-1138; CVE-2020-1139; CVE-2020-1141; CVE-2020-1143; CVE-2020-1144; CVE-2020-1146; CVE-2020-1149; CVE-2020-1152; CVE-2020-1167; CVE-2020-1172; CVE-2020-1174; CVE-2020-1175; CVE-2020-1176; CVE-2020-1179; CVE-2020-1180; CVE-2020-1184; CVE-2020-1194; CVE-2020-1196; CVE-2020-1197; CVE-2020-1202; CVE-2020-1203; CVE-2020-1207; CVE-2020-1208; CVE-2020-1211; CVE-2020-1228; CVE-2020-1230; CVE-2020-1231; CVE-2020-1232; CVE-2020-1234; CVE-2020-1235; CVE-2020-1236; CVE-2020-1239; CVE-2020-1251; CVE-2020-1252; CVE-2020-1253; CVE-2020-1254; CVE-2020-1255; CVE-2020-1256; CVE-2020-1257; CVE-2020-1258; CVE-2020-1269; CVE-2020-1270; CVE-2020-1271; CVE-2020-1272; CVE-2020-1278; CVE-2020-1279; CVE-2020-1281; CVE-2020-1282; CVE-2020-1300; CVE-2020-1301; CVE-2020-1302; CVE-2020-1304; CVE-2020-1305; CVE-2020-1308; CVE-2020-1309; CVE-2020-1310; CVE-2020-1334; CVE-2020-1336; CVE-2020-1337; CVE-2020-1339; CVE-2020-1344; CVE-2020-1348; CVE-2020-1351; CVE-2020-1352; CVE-2020-1361; CVE-2020-1362; CVE-2020-1364; CVE-2020-1365; CVE-2020-1368; CVE-2020-1369; CVE-2020-1370; CVE-2020-1371; CVE-



Tenable-Detected Vulnerability Discrepancies - Vulnerability Detail

* BigFix data

Vulnerability Title: KB4540670: Windows 10 Version 1607 and Windows Server 2016 March 20...

Plugin ID: 134369

Published Date: 3/10/2020 12:00:00 AM

CVSS: High

VPR: High

VPR Score: 10

* Fixlet Title: MS21-MAR: Cumulative Update for Windows Server 2016 - ...

* Fixlet ID: 500080303

* Fixlet Site: Patches for Windows

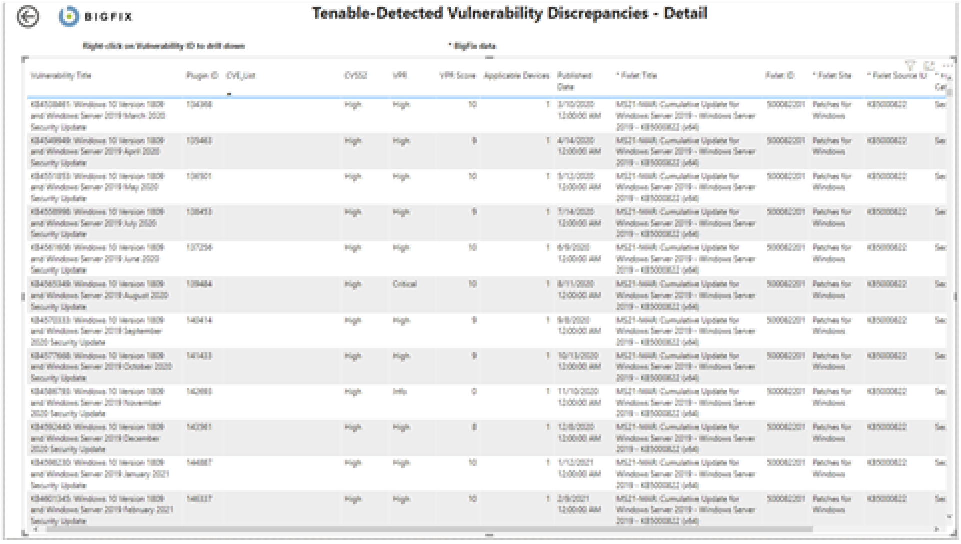
* Fixlet Source ID: KB5000803

* Fixlet Category: Security Update

* Source Release Date: 03/09/2021

Right-click on Device ID to drill down

Date Detected	* BigFix Computer ID	* Computer Name	* OS	IP Address	Device Type	Last Report Time
3/8/2021 12:00:00 AM	1088640206-1	WIN-C610KB547D8	Win2016 10.0.14393.2273 (1607)	10.134.146.134	Server	3/25/2021 4:59:16 PM



Tenable-Detected Vulnerability Discrepancies - Detail

Right-click on Vulnerability ID to drill down

* BigFix data

Vulnerability Title	Plugin ID	CVE_List	CVSS2	VPR	VPR Score	Applicable Devices	Published Date	* Fixlet Title	Fixlet ID	* Fixlet Site	* Fixlet Source ID	* Fi Cat
KB4538461: Windows 10 Version 1809 and Windows Server 2019 March 2020 Security Update	134368		High	High	10	1	3/10/2020 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4549949: Windows 10 Version 1809 and Windows Server 2019 April 2020 Security Update	135463		High	High	9	1	4/14/2020 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4551853: Windows 10 Version 1809 and Windows Server 2019 May 2020 Security Update	136501		High	High	10	1	5/12/2020 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4558998: Windows 10 Version 1809 and Windows Server 2019 July 2020 Security Update	138453		High	High	9	1	7/14/2020 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4561608: Windows 10 Version 1809 and Windows Server 2019 June 2020 Security Update	137256		High	High	10	1	6/9/2020 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4565349: Windows 10 Version 1809 and Windows Server 2019 August 2020 Security Update	139484		High	Critical	10	1	8/11/2020 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4570333: Windows 10 Version 1809 and Windows Server 2019 September 2020 Security Update	140414		High	High	9	1	9/8/2020 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4577668: Windows 10 Version 1809 and Windows Server 2019 October 2020 Security Update	141433		High	High	9	1	10/13/2020 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4586793: Windows 10 Version 1809 and Windows Server 2019 November 2020 Security Update	142693		High	Info	0	1	11/10/2020 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4592440: Windows 10 Version 1809 and Windows Server 2019 December 2020 Security Update	143561		High	High	8	1	12/8/2020 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4598230: Windows 10 Version 1809 and Windows Server 2019 January 2021 Security Update	144887		High	High	10	1	1/12/2021 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec
KB4601345: Windows 10 Version 1809 and Windows Server 2019 February 2021 Security Update	146337		High	High	10	1	2/9/2021 12:00:00 AM	MS21-MAR: Cumulative Update for Windows Server 2019 - Windows Server 2019 - KB5000822 (x64)	500082201	Patches for Windows	KB5000822	Sec

Tableau reports

Use this section to become familiar with Tableau reports.

Tableau reports for:

- Qualys
- Tenable.io
- Tenable.sc

The reports are produced in Tableau version 2020.4+.

- Reporting differences: the functionality of the reports is nearly identical between Power BI and Tableau. This section details the differences between the reports
- Navigation: each visualization is portrayed on the dashboard page. Visualizations that do not apply to your business process can be removed as necessary

- Qualys Severity

  The Severity value is provided by Qualys to measure the relative security risk associated with the vulnerability. Factors included in this measure are:

  - Possible consequences
  - Complexity
  - Likelihood that the exploit will work under normal conditions
  - Network location
  - Privileges needed by the attacker
  - Prevalence of affected software
  - Existence of known attacks

  In the IVR database, the information is stored in the vulnerabilities.severity column. The reporting aggregation tables return both the numerical score and a value (where applicable) corresponding to the following matrix:

  Table 4.

Severity Value	Level Value
1	Minimal
2	Medium
3	Serious
4	Critical
5	Urgent

  For more information regarding this topic from the vendor, please visit https://qualysguard.qualys.com/qwebhelp/fo_portal/knowledgebase/severity_levels.htm

- Tenable Severity

  The Vulnerability Priority Rating (VPR) value is provided by Tenable to measure the relative security risk associated with the vulnerability. Factors included in this measure are:

  - Vulnerability Age
  - CVSSv3 Impact Score
  - Exploit Code Maturity
  - Product Coverage
  - Threat Sources
  - Threat Intensity
  - Threat Recency

  In the IVR database, the information is stored in the vulnerabilities.vendor_rating column. The reporting aggregation tables return both the numerical score and a value (where applicable) corresponding to the following matrix:

  Table 5.

VPR Value	Level Value
9.0 – 10.0	Critical
7.0 – 8.9	High
4.0 – 6.9	Medium
0.1 – 3.9	Low

  For more information regarding this topic from the vendor, please visit https://docs.tenable.com/tenablesc/Content/RiskMetrics.htm

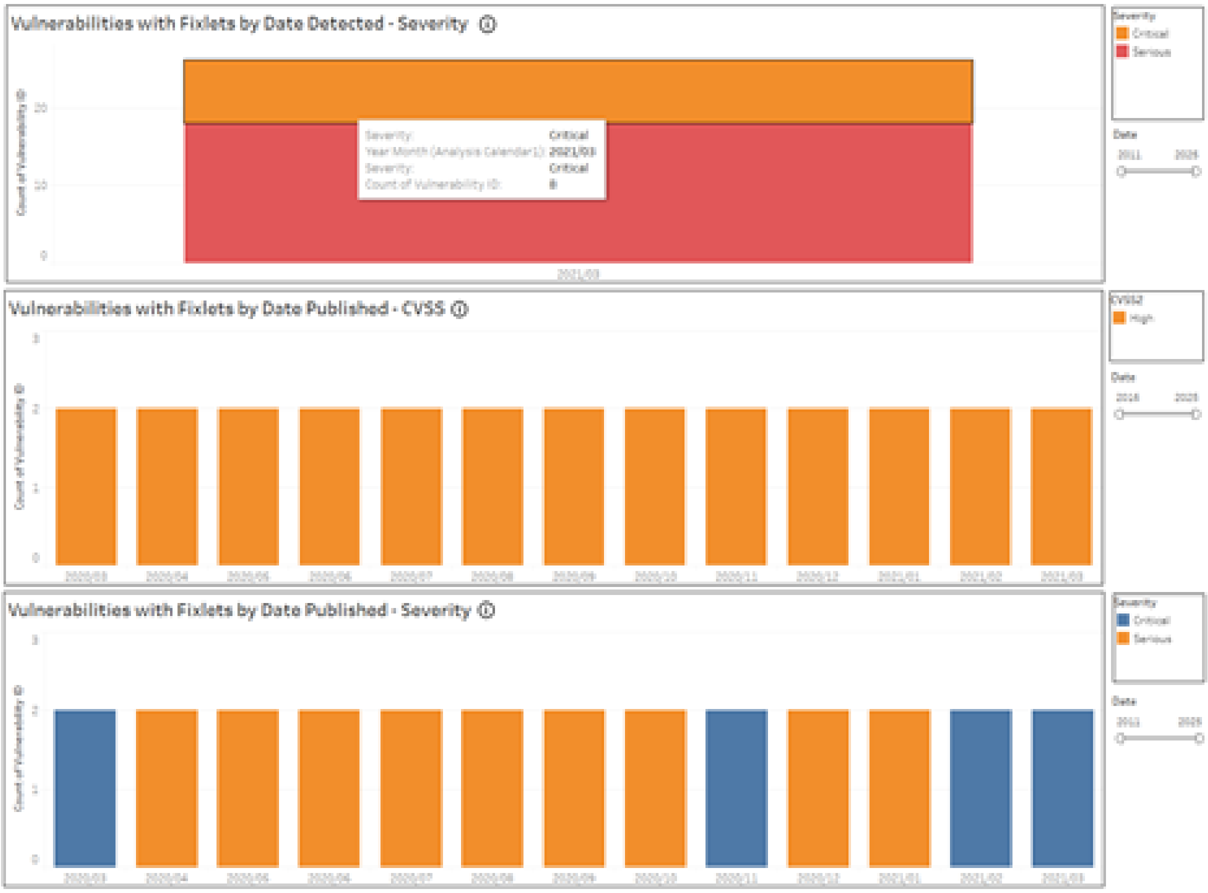
Tableau reports for Qualys

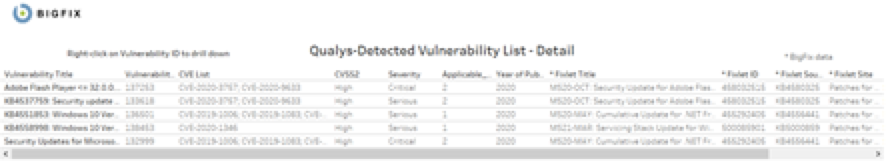
Use this section to become familiar with Tableau reports for Qualys.

Chart details:

- Vulnerability Title - vulnerability title
- Vulnerability ID - a unique identifier assigned to a vulnerability
- Device Name - name of the device
- Severity - level of risk associated with a vulnerability. Severity rating scale ranges from 1 to 5
- Detected Date - date when a vulnerability was first detected
- CVSS2 - Common Vulnerability Scoring System version 2
- Applicable Devices - devices that are affected by a vulnerability

Detected Vulnerabilities with Applicable Fixlets



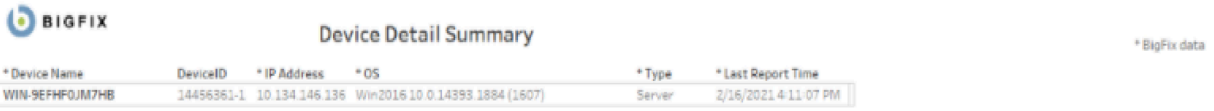


Right-click on Vulnerability ID to drill down

Qualys-Detected Vulnerability List - Detail

* BigFix data

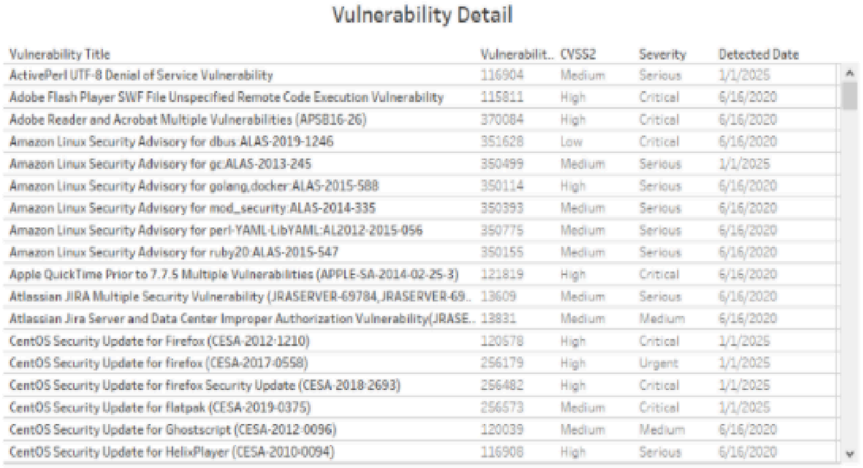
Vulnerability Title	Vulnerabilit...	CVE List	CVSS2	Severity	Applicable_...	Year of Pub...	* Fixlet Title	* Fixlet ID	* Fixlet Sou...	* Fixlet Site
Adobe Flash Player <= 32.0.0...	137253	CVE-2020-3757; CVE-2020-9633	High	Critical	2	2020	MS20-OCT: Security Update for Adobe Flas...	458032516	KB4580325	Patches for ...
KB4537759: Security update ...	133618	CVE-2020-3757; CVE-2020-9633	High	Serious	2	2020	MS20-OCT: Security Update for Adobe Flas...	458032516	KB4580325	Patches for ...
KB4551853: Windows 10 Ver...	136601	CVE-2019-1006; CVE-2019-1083; CVE-...	High	Serious	1	2020	MS20-MAY: Cumulative Update for .NET Fr...	455292405	KB4556441	Patches for ...
KB4558998: Windows 10 Ver...	138453	CVE-2020-1346	High	Serious	1	2020	MS21-MAR: Servicing Stack Update for Wi...	500000901	KB5000859	Patches for ...
Security Updates for Microso...	132999	CVE-2019-1006; CVE-2019-1083; CVE-...	High	Critical	2	2020	MS20-MAY: Cumulative Update for .NET Fr...	455292405	KB4556441	Patches for ...



Device Detail Summary

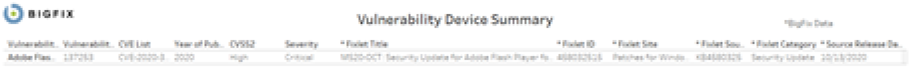
* BigFix data

* Device Name	DeviceID	* IP Address	* OS	* Type	* Last Report Time
WIN-9EFHF0JM7HB	14456361-1	10.134.146.136	Win2016 10.0.14393.1884 (1607)	Server	2/16/2021 4:11:07 PM



Vulnerability Detail

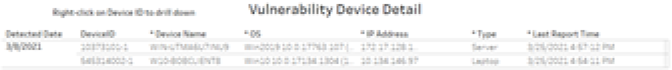
Vulnerability Title	Vulnerabilit..	CVSS2	Severity	Detected Date
ActivePerl UTF-8 Denial of Service Vulnerability	116904	Medium	Serious	1/1/2025
Adobe Flash Player SWF File Unspecified Remote Code Execution Vulnerability	115811	High	Critical	6/16/2020
Adobe Reader and Acrobat Multiple Vulnerabilities (APSB16-26)	370084	High	Critical	6/16/2020
Amazon Linux Security Advisory for dbus:ALAS-2019-1246	351628	Low	Critical	6/16/2020
Amazon Linux Security Advisory for gc:ALAS-2013-245	350499	Medium	Serious	1/1/2025
Amazon Linux Security Advisory for golang,docker:ALAS-2015-588	350114	High	Serious	6/16/2020
Amazon Linux Security Advisory for mod_security:ALAS-2014-335	350393	Medium	Serious	6/16/2020
Amazon Linux Security Advisory for perl-YAML-LibYAML:AL2012-2015-056	350775	Medium	Serious	6/16/2020
Amazon Linux Security Advisory for ruby20:ALAS-2015-547	350155	Medium	Serious	6/16/2020
Apple QuickTime Prior to 7.7.5 Multiple Vulnerabilities (APPLE-SA-2014-02-25-3)	121819	High	Critical	6/16/2020
Atlassian JIRA Multiple Security Vulnerability (JRASERVER-69784,JRASERVER-69..	13609	Medium	Serious	6/16/2020
Atlassian Jira Server and Data Center Improper Authorization Vulnerability(JRASE..	13831	Medium	Medium	6/16/2020
CentOS Security Update for Firefox (CESA-2012:1210)	120578	High	Critical	1/1/2025
CentOS Security Update for firefox (CESA-2017:0558)	256179	High	Urgent	1/1/2025
CentOS Security Update for firefox Security Update (CESA-2018:2693)	256482	High	Critical	1/1/2025
CentOS Security Update for flatpak (CESA-2019:0375)	256573	Medium	Critical	1/1/2025
CentOS Security Update for Ghostscript (CESA-2012:0096)	120039	Medium	Medium	6/16/2020
CentOS Security Update for HelixPlayer (CESA-2010:0094)	116908	High	Serious	6/16/2020



Vulnerability Device Summary

*BigFix Data

Vulnerabilit..	Vulnerabilit..	CVE List	Year of Pub..	CVSS2	Severity	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Release De..
Adobe Flas..	137263	CVE-2020-3..	2020	High	Critical	MS20-OCT: Security Update for Adobe Flash Player fo..	458032515	Patches for Windo..	KB4580325	Security Update	10/13/2020

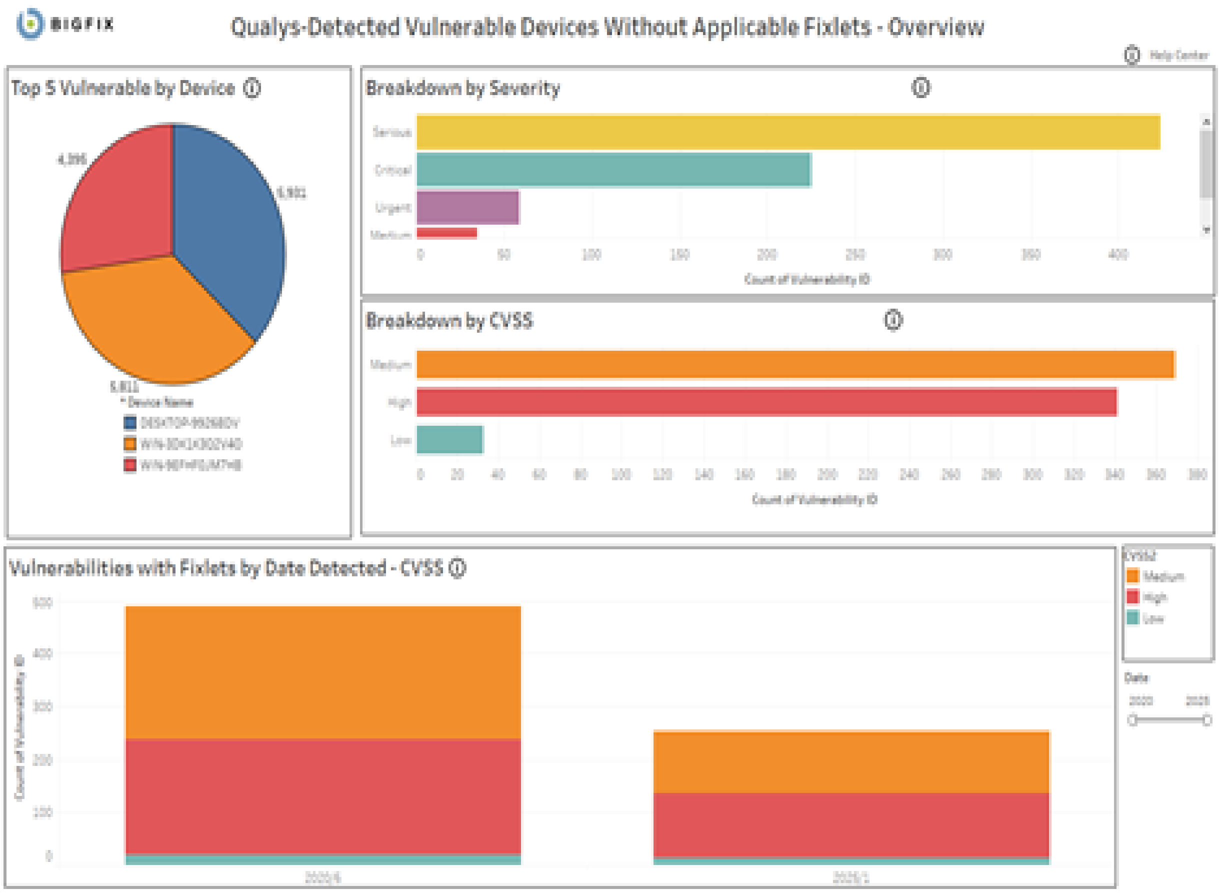


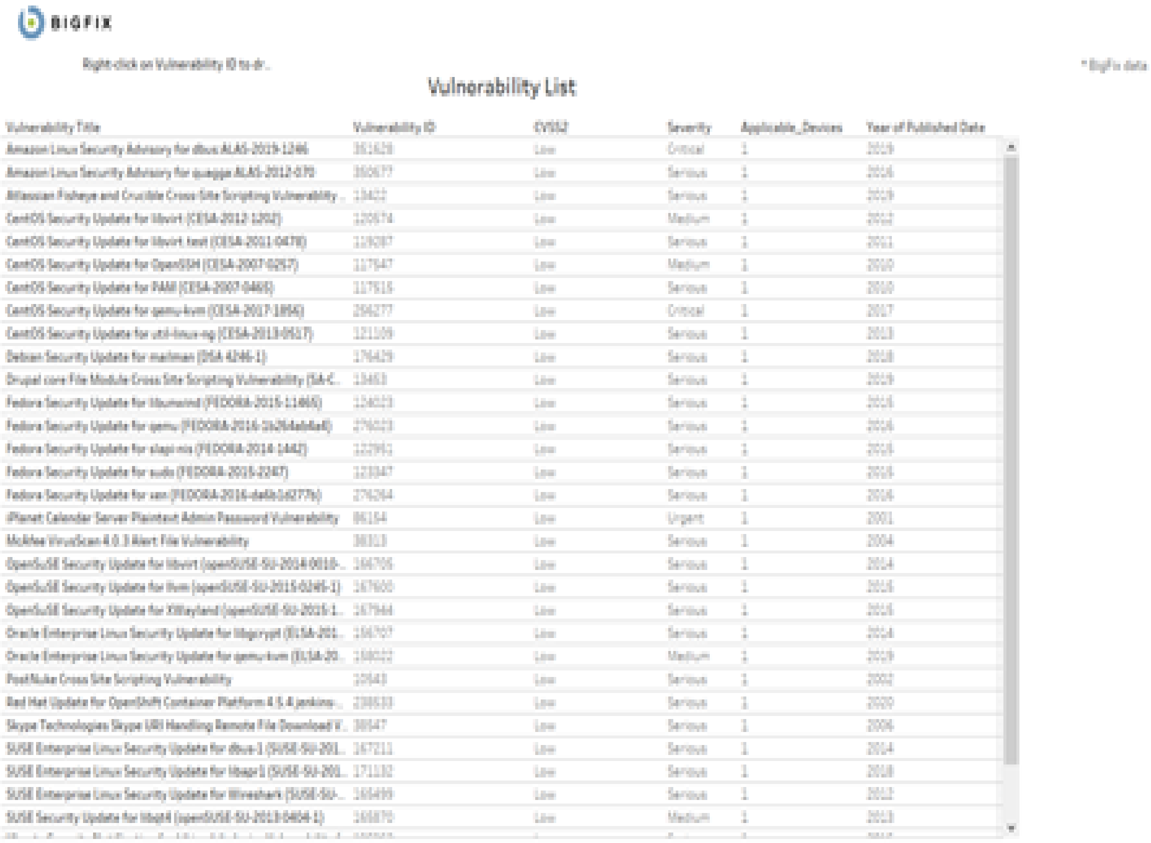
Right-click on Device ID to drill down

Vulnerability Device Detail

Detected Date	DeviceID	* Device Name	* OS	* IP Address	* Type	* Last Report Time
3/8/2021	10373101-1	WIN-GTM66UTNU9	Win2019 10.0.17763.107 (..	172.17.128.1..	Server	3/25/2021 4:57:12 PM
	545314002-1	W10-BOBCLIENT8	Win10 10.0.17134.1304 (1..	10.134.146.97	Laptop	3/25/2021 4:54:11 PM

Detected Vulnerabilities without Available Fixlets



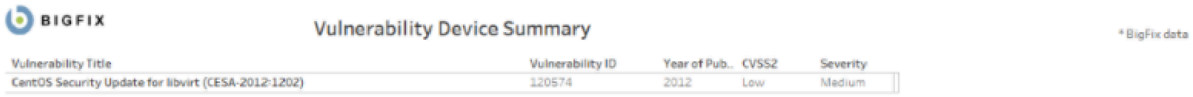


Right-click on Vulnerability ID to dr...

* BigFix data

Vulnerability List

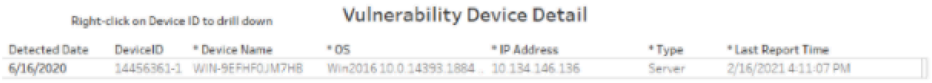
Vulnerability Title	Vulnerability ID	CVSS2	Severity	Applicable_Devices	Year of Published Date
Amazon Linux Security Advisory for dbus: ALAS-2019-1246	351628	Low	Critical	1	2019
Amazon Linux Security Advisory for quagga: ALAS-2012-070	350677	Low	Serious	1	2016
Atlassian Fisheye and Crucible Cross Site Scripting Vulnerability ...	13422	Low	Serious	1	2019
CentOS Security Update for libvirt (CESA-2012:1202)	120574	Low	Medium	1	2012
CentOS Security Update for libvirt, test (CESA-2011:0478)	119087	Low	Serious	1	2011
CentOS Security Update for OpenSSH (CESA-2007:0257)	117547	Low	Medium	1	2010
CentOS Security Update for PAM (CESA-2007:0465)	117516	Low	Serious	1	2010
CentOS Security Update for qemu-kvm (CESA-2017:1856)	256277	Low	Critical	1	2017
CentOS Security Update for util-linux-ng (CESA-2013:0517)	121109	Low	Serious	1	2013
Debian Security Update for mailman (DSA 4246-1)	176429	Low	Serious	1	2018
Drupal core File Module Cross Site Scripting Vulnerability (SA-C...	13453	Low	Serious	1	2019
Fedora Security Update for libmaxmind (FEDORA-2015-11465)	124023	Low	Serious	1	2016
Fedora Security Update for qemu (FEDORA-2016-1b26dab6a8)	276023	Low	Serious	1	2016
Fedora Security Update for slapi-nis (FEDORA-2014-1442)	122951	Low	Serious	1	2016
Fedora Security Update for sudo (FEDORA-2015-2247)	123047	Low	Serious	1	2016
Fedora Security Update for xen (FEDORA-2016-da6b1d277b)	276264	Low	Serious	1	2016
iPlanet Calendar Server Plaintext Admin Password Vulnerability	86154	Low	Urgent	1	2001
McAfee VirusScan 4.0.3 Alert File Vulnerability	38313	Low	Serious	1	2004
OpenSuSE Security Update for libvirt (openSUSE-SU-2014:0010-...	166705	Low	Serious	1	2014
OpenSuSE Security Update for llvm (openSUSE-SU-2015:0245-1)	167600	Low	Serious	1	2016
OpenSuSE Security Update for XWayland (openSUSE-SU-2015:1...	167944	Low	Serious	1	2016
Oracle Enterprise Linux Security Update for libgcrypt (ELSA-201...	166707	Low	Serious	1	2014
Oracle Enterprise Linux Security Update for qemu-kvm (ELSA-20...	158022	Low	Medium	1	2019
PostNuke Cross Site Scripting Vulnerability	10543	Low	Serious	1	2002
Red Hat Update for OpenShift Container Platform 4.5.4 jenkins...	238633	Low	Serious	1	2020
Skype Technologies Skype URI Handling Remote File Download V...	38547	Low	Serious	1	2006
SUSE Enterprise Linux Security Update for dbus-1 (SUSE-SU-201...	167211	Low	Serious	1	2014
SUSE Enterprise Linux Security Update for libapr1 (SUSE-SU-201...	171132	Low	Serious	1	2018
SUSE Enterprise Linux Security Update for Wireshark (SUSE-SU-...	165499	Low	Serious	1	2012
SUSE Security Update for libqt4 (openSUSE-SU-2013:0404-1)	165870	Low	Medium	1	2013
[illegible]	[illegible]	[illegible]	[illegible]	1	[illegible]



Vulnerability Device Summary

* BigFix data

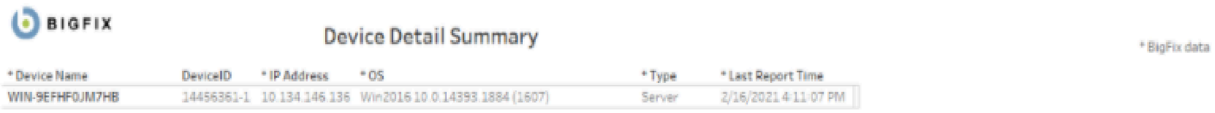
Vulnerability Title	Vulnerability ID	Year of Pub..	CVSS2	Severity
CentOS Security Update for libvirt (CESA-2012:1202)	120574	2012	Low	Medium



Right-click on Device ID to drill down

Vulnerability Device Detail

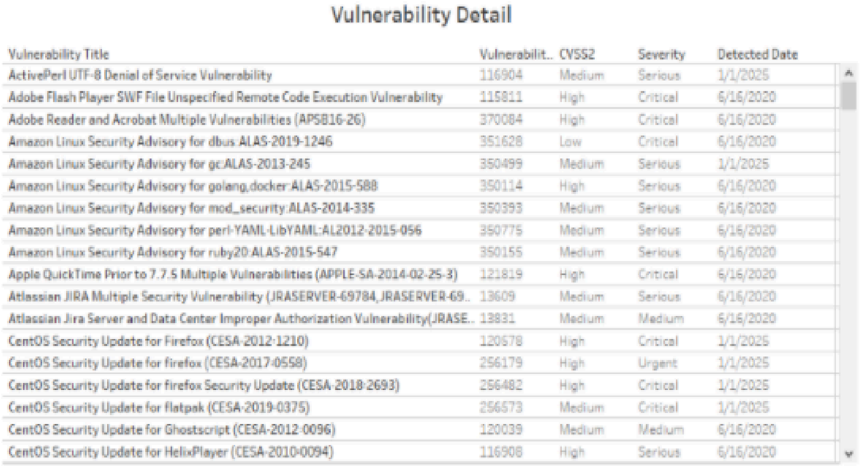
Detected Date	DeviceID	* Device Name	* OS	* IP Address	* Type	* Last Report Time
6/16/2020	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 ..	10.134.146.136	Server	2/16/2021 4:11:07 PM



Device Detail Summary

* BigFix data

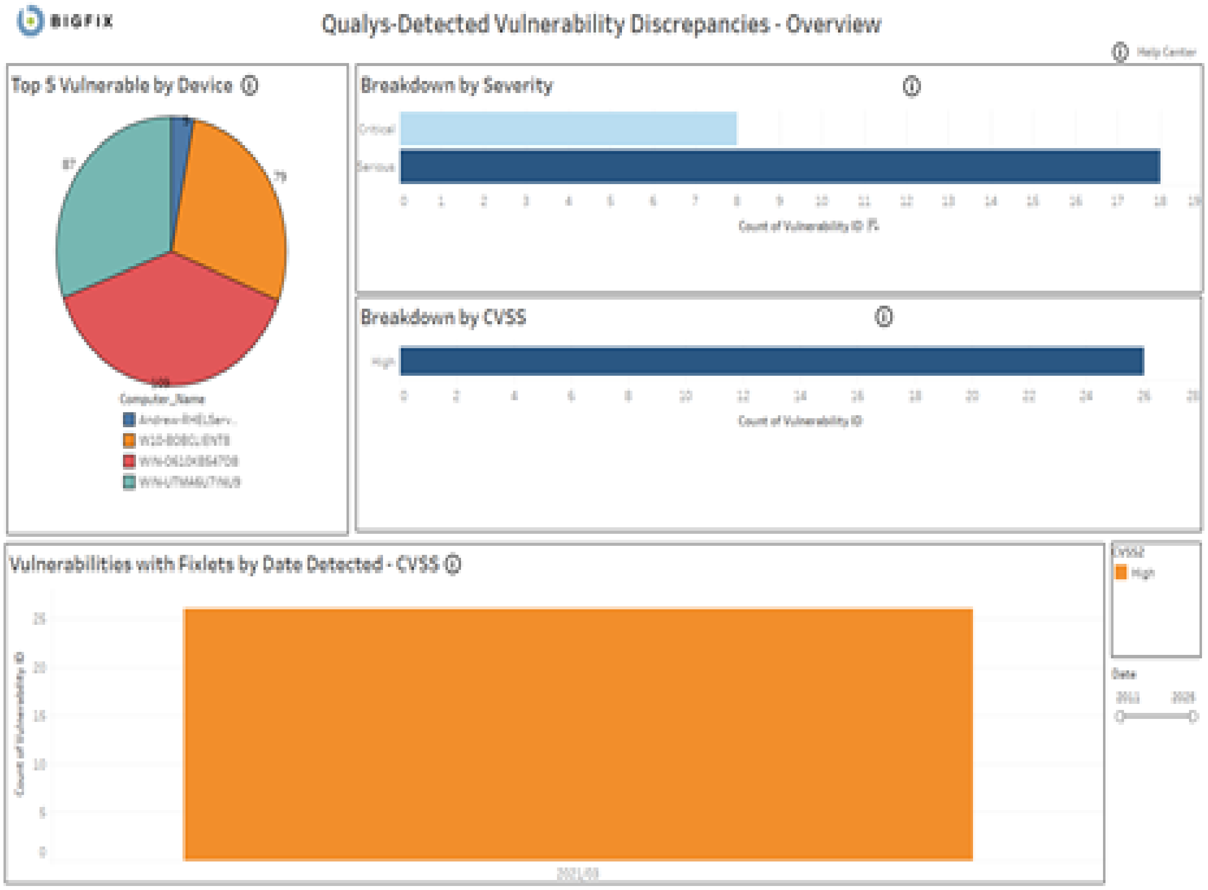
* Device Name	DeviceID	* IP Address	* OS	* Type	* Last Report Time
WIN-9EFHF0JM7HB	14456361-1	10.134.146.136	Win2016 10.0.14393.1884 (1607)	Server	2/16/2021 4:11:07 PM

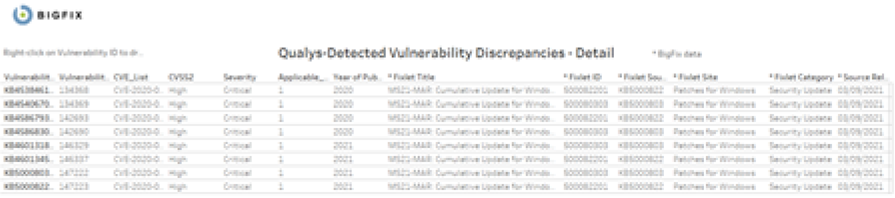


Vulnerability Detail

Vulnerability Title	Vulnerabilit..	CVSS2	Severity	Detected Date
ActivePerl UTF-8 Denial of Service Vulnerability	116904	Medium	Serious	1/1/2025
Adobe Flash Player SWF File Unspecified Remote Code Execution Vulnerability	115811	High	Critical	6/16/2020
Adobe Reader and Acrobat Multiple Vulnerabilities (APSB16-26)	370084	High	Critical	6/16/2020
Amazon Linux Security Advisory for dbus:ALAS-2019-1246	351628	Low	Critical	6/16/2020
Amazon Linux Security Advisory for gc:ALAS-2013-245	350499	Medium	Serious	1/1/2025
Amazon Linux Security Advisory for golang,docker:ALAS-2015-588	350114	High	Serious	6/16/2020
Amazon Linux Security Advisory for mod_security:ALAS-2014-335	350393	Medium	Serious	6/16/2020
Amazon Linux Security Advisory for perl-YAML-LibYAML:AL2012-2015-056	350775	Medium	Serious	6/16/2020
Amazon Linux Security Advisory for ruby20:ALAS-2015-547	350155	Medium	Serious	6/16/2020
Apple QuickTime Prior to 7.7.5 Multiple Vulnerabilities (APPLE-SA-2014-02-25-3)	121819	High	Critical	6/16/2020
Atlassian JIRA Multiple Security Vulnerability (JRASERVER-69784,JRASERVER-69..	13609	Medium	Serious	6/16/2020
Atlassian Jira Server and Data Center Improper Authorization Vulnerability(JRASE..	13831	Medium	Medium	6/16/2020
CentOS Security Update for Firefox (CESA-2012-1210)	120578	High	Critical	1/1/2025
CentOS Security Update for firefox (CESA-2017-0558)	256179	High	Urgent	1/1/2025
CentOS Security Update for firefox Security Update (CESA-2018-2693)	256482	High	Critical	1/1/2025
CentOS Security Update for flatpak (CESA-2019-0375)	256573	Medium	Critical	1/1/2025
CentOS Security Update for Ghostscript (CESA-2012-0096)	120039	Medium	Medium	6/16/2020
CentOS Security Update for HelixPlayer (CESA-2010-0094)	116908	High	Serious	6/16/2020

Vulnerability Discrepancies





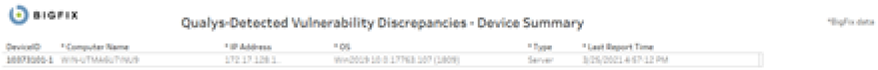
BIGFIX

Right-click on Vulnerability ID to dr..

Qualys-Detected Vulnerability Discrepancies - Detail

* BigFix data

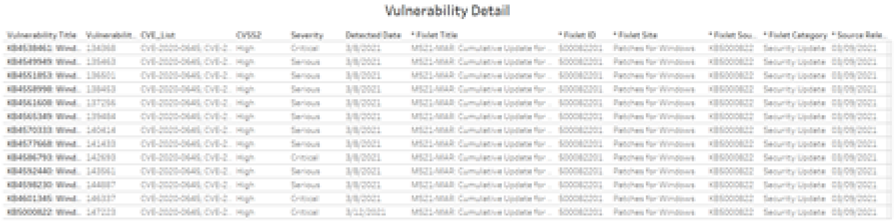
Vulnerabilit..	Vulnerabilit..	CVE_List	CVSS2	Severity	Applicable_..	Year of Pub..	* Fixlet Title	* Fixlet ID	* Fixlet Sou..	* Fixlet Site	* Fixlet Category	* Source Rel..
KB4538461..	134368	CVE-2020-0..	High	Critical	1	2020	MS21-MAR: Cumulative Update for Windo..	500082201	KB5000822	Patches for Windows	Security Update	03/09/2021
KB4540670..	134369	CVE-2020-0..	High	Critical	1	2020	MS21-MAR: Cumulative Update for Windo..	500080303	KB5000803	Patches for Windows	Security Update	03/09/2021
KB4586793..	142693	CVE-2020-0..	High	Critical	1	2020	MS21-MAR: Cumulative Update for Windo..	500082201	KB5000822	Patches for Windows	Security Update	03/09/2021
KB4586830..	142690	CVE-2020-0..	High	Critical	1	2020	MS21-MAR: Cumulative Update for Windo..	500080303	KB5000803	Patches for Windows	Security Update	03/09/2021
KB4601318..	146329	CVE-2020-0..	High	Critical	1	2021	MS21-MAR: Cumulative Update for Windo..	500080303	KB5000803	Patches for Windows	Security Update	03/09/2021
KB4601345..	146337	CVE-2020-0..	High	Critical	1	2021	MS21-MAR: Cumulative Update for Windo..	500082201	KB5000822	Patches for Windows	Security Update	03/09/2021
KB5000803..	147222	CVE-2020-0..	High	Critical	1	2021	MS21-MAR: Cumulative Update for Windo..	500080303	KB5000803	Patches for Windows	Security Update	03/09/2021
KB5000822..	147223	CVE-2020-0..	High	Critical	1	2021	MS21-MAR: Cumulative Update for Windo..	500082201	KB5000822	Patches for Windows	Security Update	03/09/2021



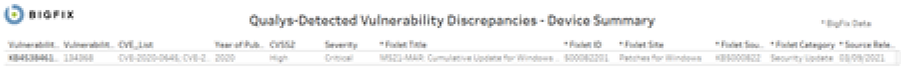
Qualys-Detected Vulnerability Discrepancies - Device Summary

*BigFix data

DeviceID	* Computer Name	* IP Address	* OS	* Type	* Last Report Time
10073101-1	WIN-UTMA6U7INU9	172.17.128.1..	Win2019 10.0.17763.107 (1809)	Server	3/25/2021 4:57:12 PM


Vulnerability Detail

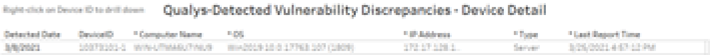
Vulnerability Title	Vulnerabilit..	CVE_List	CVSS2	Severity	Detected Date	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Rele..
KB4538461: Wind..	134368	CVE-2020-0645, CVE-2..	High	Critical	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4549949: Wind..	135463	CVE-2020-0645, CVE-2..	High	Serious	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4551853: Wind..	136501	CVE-2020-0645, CVE-2..	High	Serious	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4558998: Wind..	138463	CVE-2020-0645, CVE-2..	High	Serious	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4561608: Wind..	137256	CVE-2020-0645, CVE-2..	High	Serious	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4565349: Wind..	139484	CVE-2020-0645, CVE-2..	High	Serious	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4570333: Wind..	140414	CVE-2020-0645, CVE-2..	High	Serious	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4577668: Wind..	141433	CVE-2020-0645, CVE-2..	High	Serious	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4586793: Wind..	142693	CVE-2020-0645, CVE-2..	High	Critical	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4592440: Wind..	143561	CVE-2020-0645, CVE-2..	High	Serious	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4598230: Wind..	144887	CVE-2020-0645, CVE-2..	High	Serious	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4601345: Wind..	146337	CVE-2020-0645, CVE-2..	High	Critical	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB5000822: Wind..	147223	CVE-2020-0645, CVE-2..	High	Critical	3/11/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021



Qualys-Detected Vulnerability Discrepancies - Device Summary

* BigFix Data

Vulnerabilit..	Vulnerabilit..	CVE_List	Year of Pub..	CVSS2	Severity	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Rele..
KB4538461..	134368	CVE-2020-0645; CVE-2..	2020	High	Critical	MS21-MAR: Cumulative Update for Windows ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021


Right-click on Device ID to drill down

Qualys-Detected Vulnerability Discrepancies - Device Detail

Detected Date	DeviceID	* Computer Name	* OS	* IP Address	* Type	* Last Report Time
3/8/2021	10073101-1	WIN-UTMA6U7INU9	Win2019 10.0.17763.107 (1809)	172.17.128.1..	Server	3/25/2021 4:57:12 PM

Tableau reports for Tenable.io

Use this section to become familiar with Tableau reports for Tenable.io

BigFix Insights for Vulnerability Remediation can now also consume vulnerability data from Tenable.io. With Tenable Lumin available, BigFix Insights for Vulnerability Remediation also consumes asset prioritization data:

- Asset Criticality Rating (ACR): 1-10 rating that represents the asset's relative criticality based on device type, device purpose, and network location/proximity to the Internet.
- Asset Exposure Score (AES): A metric that combines ACR & VPR (Vulnerability Priority Rating) into a single score to represent an asset's relative exposure.

Refer to the link for more information: Lumin Metrics

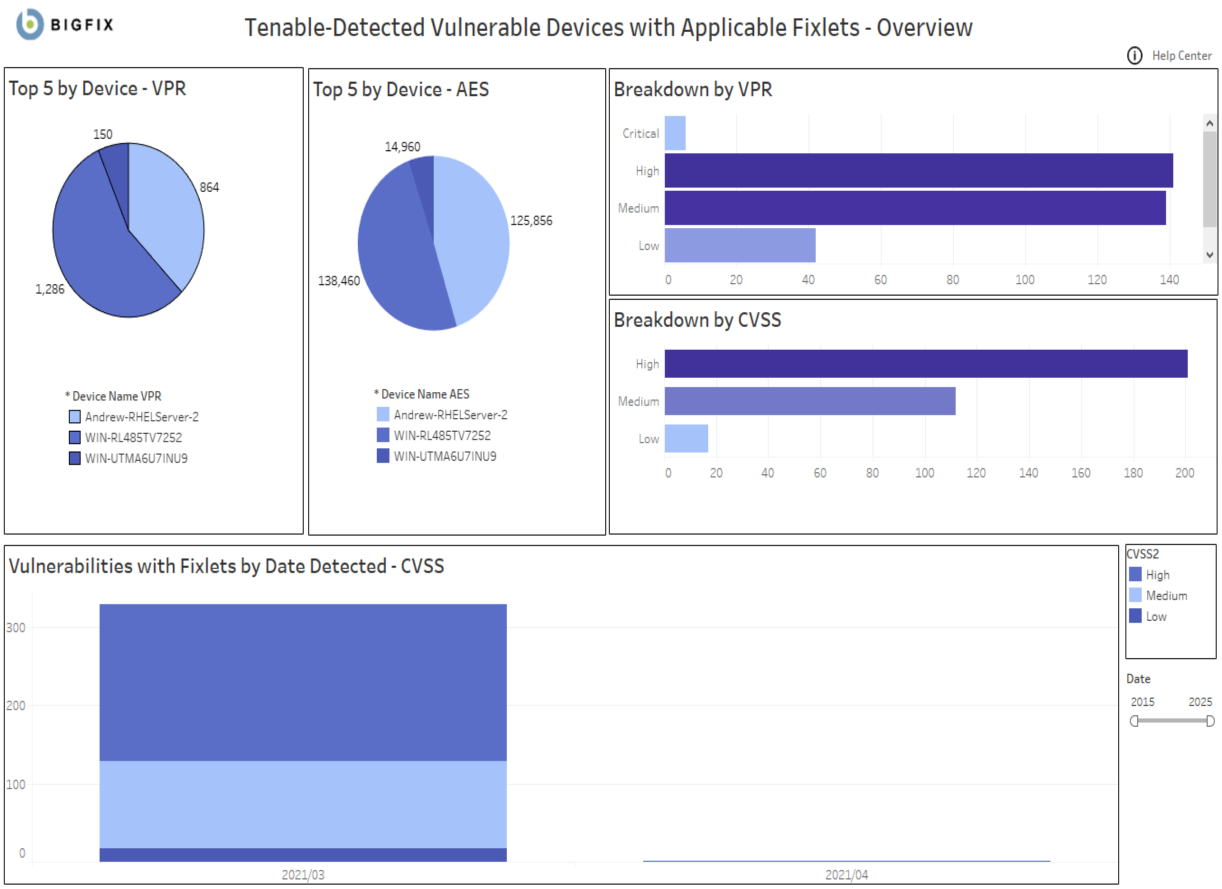
Additionally, uniquely for Tenable.io, BigFix sends its endpoint asset data to Tenable.io to give it visibility into potentially unmanaged assets.

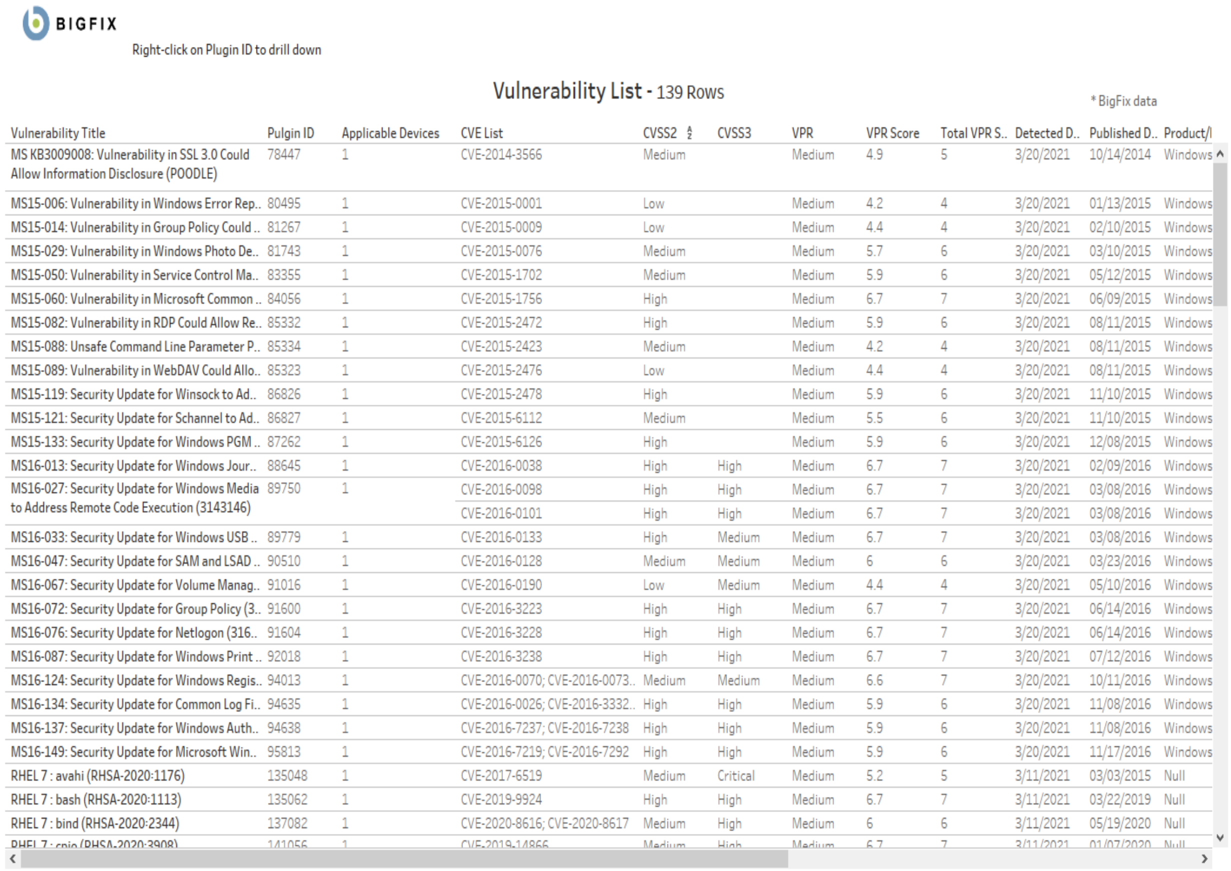
Chart details:

- Vulnerability Title - Vulnerability title
- PluginID - a unique identifier assigned to a vulnerability detection

- Applicable Devices - devices that have been scanned by Tenable and for which vulnerabilities have been identified
- CVE List - list of CVE
- CVSS2 - (Common Vulnerability Scoring System version 2), scoring system used to assess the severity and potential impact of security vulnerabilities.
- CVSS3 - (Common Vulnerability Scoring System version 3), updated version of the scoring system
- VPR - Vulnerability Priority Rating
- VPR Score - numerical value ranging from 0 to 10, with 10 being the highest priority
- Detected Date - the date when a vulnerability was first detected
- Published Date - date when the information about a vulnerability was first available
- ACR - Asset Criticality Rating: 1-10 rating that represents the asset's relative criticality based on device type, device purpose, and network location/proximity to the Internet.
- AES - Asset Exposure Score: A metric that combines ACR & VPR (Vulnerability Priority Rating) into a single score to represent an asset's relative exposure.

Detected Vulnerabilities with Applicable Fixlets



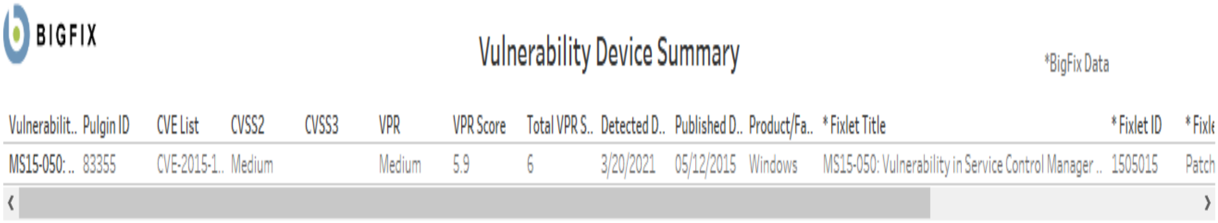


Right-click on Plugin ID to drill down

Vulnerability List - 139 Rows

* BigFix data

Vulnerability Title	Pulgin ID	Applicable Devices	CVE List	CVSS2	CVSS3	VPR	VPR Score	Total VPR S..	Detected D..	Published D..	Product/I
MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	78447	1	CVE-2014-3566	Medium		Medium	4.9	5	3/20/2021	10/14/2014	Windows
MS15-006: Vulnerability in Windows Error Rep..	80495	1	CVE-2015-0001	Low		Medium	4.2	4	3/20/2021	01/13/2015	Windows
MS15-014: Vulnerability in Group Policy Could ..	81267	1	CVE-2015-0009	Low		Medium	4.4	4	3/20/2021	02/10/2015	Windows
MS15-029: Vulnerability in Windows Photo De..	81743	1	CVE-2015-0076	Medium		Medium	5.7	6	3/20/2021	03/10/2015	Windows
MS15-050: Vulnerability in Service Control Ma..	83355	1	CVE-2015-1702	Medium		Medium	5.9	6	3/20/2021	05/12/2015	Windows
MS15-060: Vulnerability in Microsoft Common ..	84056	1	CVE-2015-1756	High		Medium	6.7	7	3/20/2021	06/09/2015	Windows
MS15-082: Vulnerability in RDP Could Allow Re..	85332	1	CVE-2015-2472	High		Medium	5.9	6	3/20/2021	08/11/2015	Windows
MS15-088: Unsafe Command Line Parameter P..	85334	1	CVE-2015-2423	Medium		Medium	4.2	4	3/20/2021	08/11/2015	Windows
MS15-089: Vulnerability in WebDAV Could Allo..	85323	1	CVE-2015-2476	Low		Medium	4.4	4	3/20/2021	08/11/2015	Windows
MS15-119: Security Update for Winsock to Ad..	86826	1	CVE-2015-2478	High		Medium	5.9	6	3/20/2021	11/10/2015	Windows
MS15-121: Security Update for Schannel to Ad..	86827	1	CVE-2015-6112	Medium		Medium	5.5	6	3/20/2021	11/10/2015	Windows
MS15-133: Security Update for Windows PGM ..	87262	1	CVE-2015-6126	High		Medium	5.9	6	3/20/2021	12/08/2015	Windows
MS16-013: Security Update for Windows Jour..	88645	1	CVE-2016-0038	High	High	Medium	6.7	7	3/20/2021	02/09/2016	Windows
MS16-027: Security Update for Windows Media to Address Remote Code Execution (3143146)	89750	1	CVE-2016-0098	High	High	Medium	6.7	7	3/20/2021	03/08/2016	Windows
			CVE-2016-0101	High	High	Medium	6.7	7	3/20/2021	03/08/2016	Windows
MS16-033: Security Update for Windows USB ..	89779	1	CVE-2016-0133	High	Medium	Medium	6.7	7	3/20/2021	03/08/2016	Windows
MS16-047: Security Update for SAM and LSAD ..	90510	1	CVE-2016-0128	Medium	Medium	Medium	6	6	3/20/2021	03/23/2016	Windows
MS16-067: Security Update for Volume Manag..	91016	1	CVE-2016-0190	Low	Medium	Medium	4.4	4	3/20/2021	05/10/2016	Windows
MS16-072: Security Update for Group Policy (3..	91600	1	CVE-2016-3223	High	High	Medium	6.7	7	3/20/2021	06/14/2016	Windows
MS16-076: Security Update for Netlogon (316..	91604	1	CVE-2016-3228	High	High	Medium	6.7	7	3/20/2021	06/14/2016	Windows
MS16-087: Security Update for Windows Print ..	92018	1	CVE-2016-3238	High	High	Medium	6.7	7	3/20/2021	07/12/2016	Windows
MS16-124: Security Update for Windows Regis..	94013	1	CVE-2016-0070; CVE-2016-0073..	Medium	Medium	Medium	6.6	7	3/20/2021	10/11/2016	Windows
MS16-134: Security Update for Common Log Fi..	94635	1	CVE-2016-0026; CVE-2016-3332..	High	High	Medium	5.9	6	3/20/2021	11/08/2016	Windows
MS16-137: Security Update for Windows Auth..	94638	1	CVE-2016-7237; CVE-2016-7238	High	High	Medium	5.9	6	3/20/2021	11/08/2016	Windows
MS16-149: Security Update for Microsoft Win..	95813	1	CVE-2016-7219; CVE-2016-7292	High	High	Medium	5.9	6	3/20/2021	11/17/2016	Windows
RHEL 7 : avahi (RHSA-2020:1176)	135048	1	CVE-2017-6519	Medium	Critical	Medium	5.2	5	3/11/2021	03/03/2015	Null
RHEL 7 : bash (RHSA-2020:1113)	135062	1	CVE-2019-9924	High	High	Medium	6.7	7	3/11/2021	03/22/2019	Null
RHEL 7 : bind (RHSA-2020:2344)	137082	1	CVE-2020-8616; CVE-2020-8617	Medium	High	Medium	6	6	3/11/2021	05/19/2020	Null
RHEL 7 : cpio (RHSA-2020:3908)	141056	1	CVE-2019-14866	Medium	High	Medium	6.7	7	3/11/2021	01/07/2020	Null

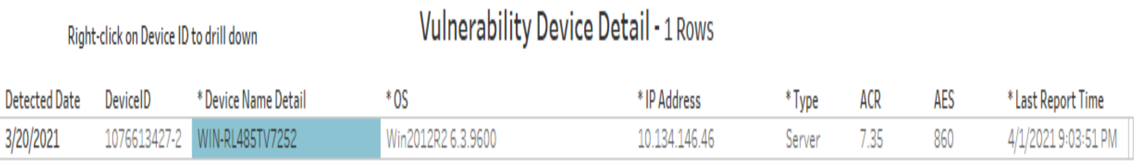


BIGFIX

Vulnerability Device Summary

*BigFix Data

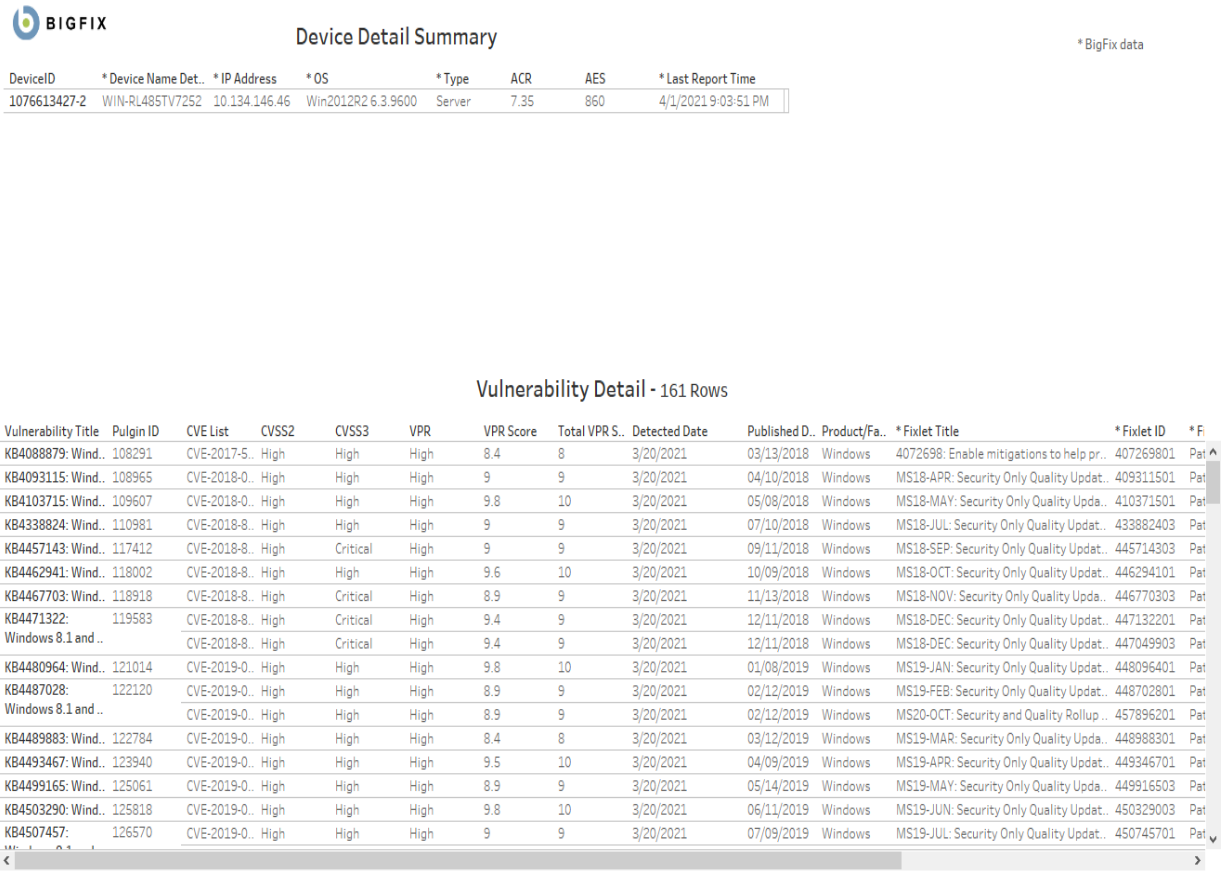
Vulnerabilit..	Pulgin ID	CVE List	CVSS2	CVSS3	VPR	VPR Score	Total VPR S..	Detected D..	Published D..	Product/Fa..	* Fixlet Title	* Fixlet ID	* Fixle
MS15-050: ..	83355	CVE-2015-1..	Medium		Medium	5.9	6	3/20/2021	05/12/2015	Windows	MS15-050: Vulnerability in Service Control Manager ..	1505015	Patch



Right-click on Device ID to drill down

Vulnerability Device Detail - 1 Rows

Detected Date	DeviceID	* Device Name Detail	* OS	* IP Address	* Type	ACR	AES	* Last Report Time
3/20/2021	1076613427-2	WIN-RL485TV7252	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM



BIGFIX

Device Detail Summary

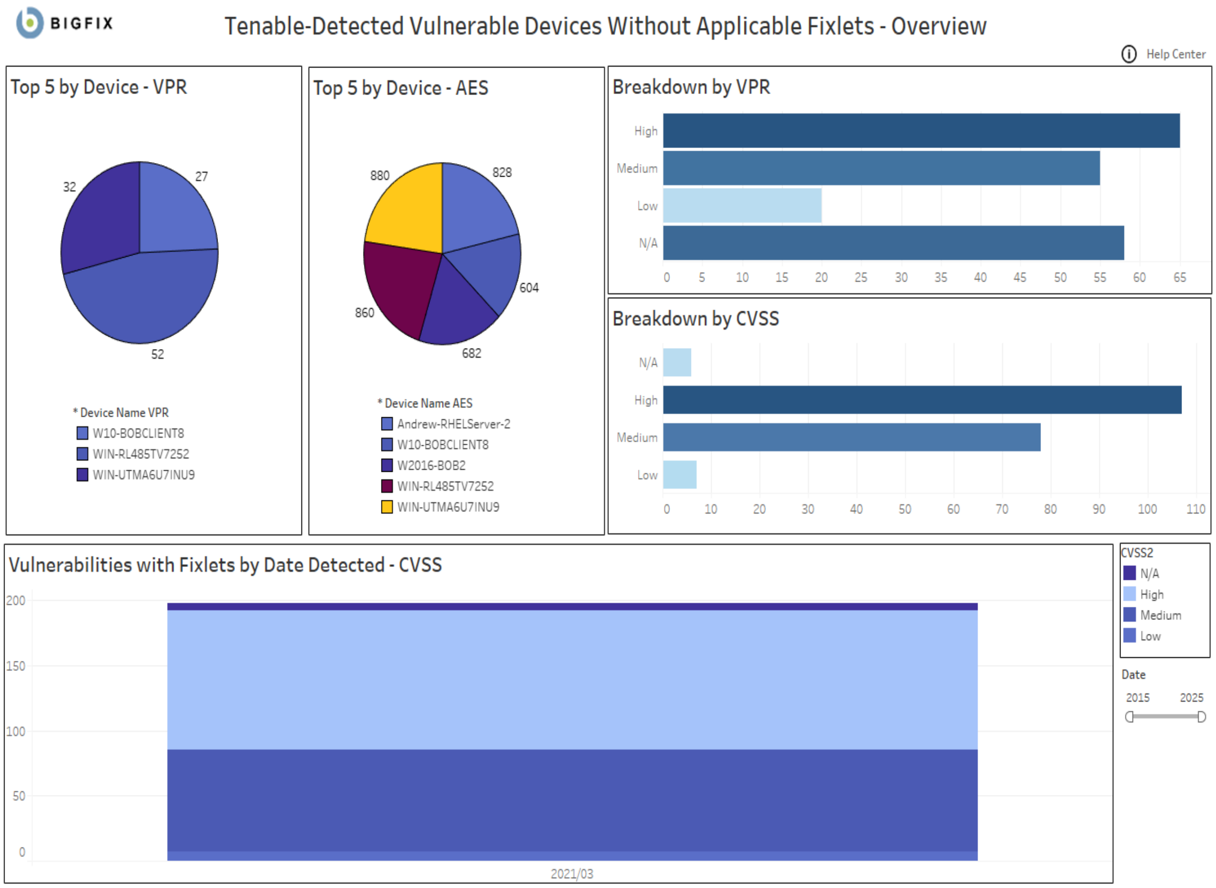
* BigFix data

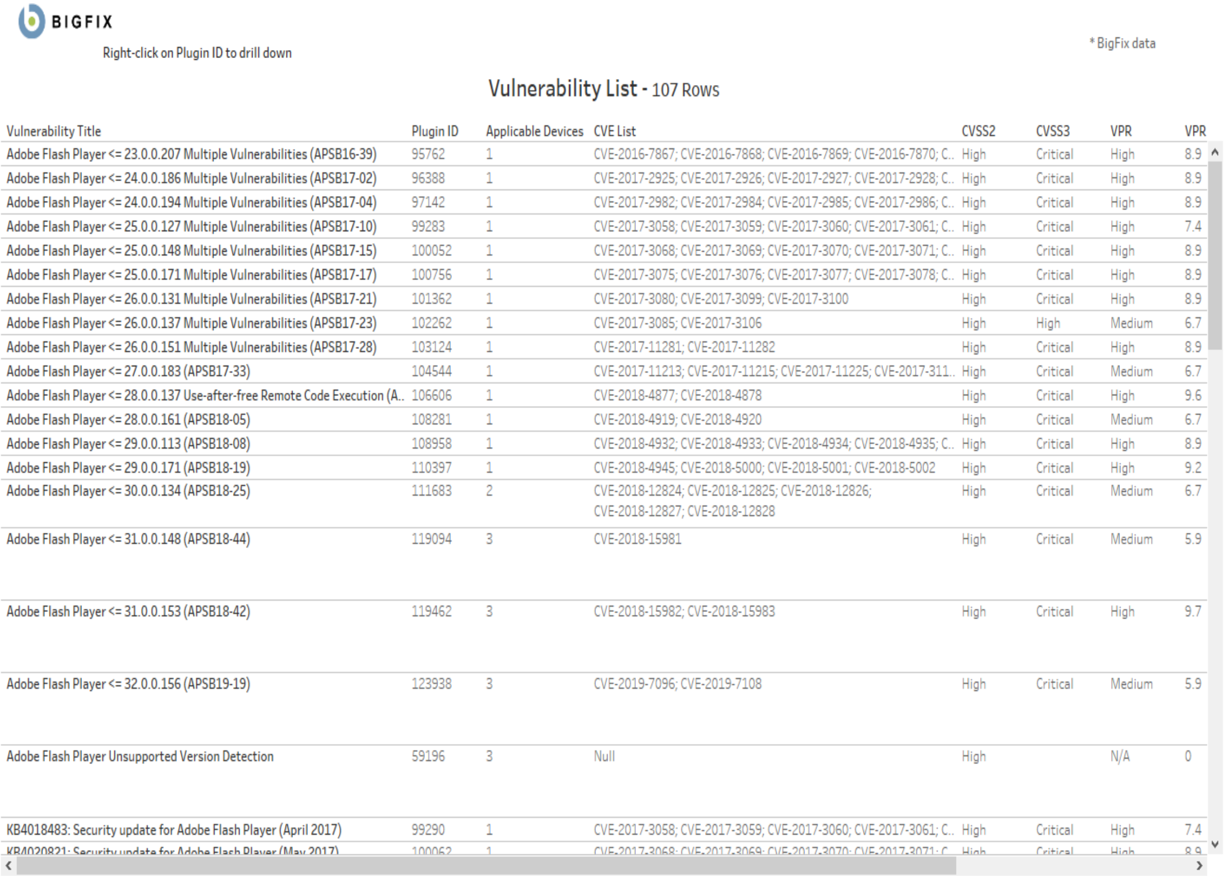
DeviceID	* Device Name Det..	* IP Address	* OS	* Type	ACR	AES	* Last Report Time
1076613427-2	WIN-RL485TV7252	10.134.146.46	Win2012R2 6.3.9600	Server	7.35	860	4/1/2021 9:03:51 PM

Vulnerability Detail - 161 Rows

Vulnerability Title	Pulgin ID	CVE List	CVSS2	CVSS3	VPR	VPR Score	Total VPR S..	Detected Date	Published D..	Product/Fa..	* Fixlet Title	* Fixlet ID	* Fi
KB4088879: Wind..	108291	CVE-2017-5..	High	High	High	8.4	8	3/20/2021	03/13/2018	Windows	4072698: Enable mitigations to help pr..	407269801	Pat
KB4093115: Wind..	108965	CVE-2018-0..	High	High	High	9	9	3/20/2021	04/10/2018	Windows	MS18-APR: Security Only Quality Updat..	409311501	Pat
KB4103715: Wind..	109607	CVE-2018-0..	High	High	High	9.8	10	3/20/2021	05/08/2018	Windows	MS18-MAY: Security Only Quality Upda..	410371501	Pat
KB4338824: Wind..	110981	CVE-2018-8..	High	High	High	9	9	3/20/2021	07/10/2018	Windows	MS18-JUL: Security Only Quality Updat..	433882403	Pat
KB4457143: Wind..	117412	CVE-2018-8..	High	Critical	High	9	9	3/20/2021	09/11/2018	Windows	MS18-SEP: Security Only Quality Updat..	445714303	Pat
KB4462941: Wind..	118002	CVE-2018-8..	High	High	High	9.6	10	3/20/2021	10/09/2018	Windows	MS18-OCT: Security Only Quality Updat..	446294101	Pat
KB4467703: Wind..	118918	CVE-2018-8..	High	Critical	High	8.9	9	3/20/2021	11/13/2018	Windows	MS18-NOV: Security Only Quality Upda..	446770303	Pat
KB4471322: Windows 8.1 and ..	119583	CVE-2018-8..	High	Critical	High	9.4	9	3/20/2021	12/11/2018	Windows	MS18-DEC: Security Only Quality Updat..	447132201	Pat
		CVE-2018-8..	High	Critical	High	9.4	9	3/20/2021	12/11/2018	Windows	MS18-DEC: Security Only Quality Updat..	447049903	Pat
KB4480964: Wind..	121014	CVE-2019-0..	High	High	High	9.8	10	3/20/2021	01/08/2019	Windows	MS19-JAN: Security Only Quality Updat..	448096401	Pat
KB4487028: Windows 8.1 and ..	122120	CVE-2019-0..	High	High	High	8.9	9	3/20/2021	02/12/2019	Windows	MS19-FEB: Security Only Quality Updat..	448702801	Pat
		CVE-2019-0..	High	High	High	8.9	9	3/20/2021	02/12/2019	Windows	MS20-OCT: Security and Quality Rollup ..	457896201	Pat
KB4489883: Wind..	122784	CVE-2019-0..	High	High	High	8.4	8	3/20/2021	03/12/2019	Windows	MS19-MAR: Security Only Quality Upda..	448988301	Pat
KB4493467: Wind..	123940	CVE-2019-0..	High	High	High	9.5	10	3/20/2021	04/09/2019	Windows	MS19-APR: Security Only Quality Updat..	449346701	Pat
KB4499165: Wind..	125061	CVE-2019-0..	High	High	High	8.9	9	3/20/2021	05/14/2019	Windows	MS19-MAY: Security Only Quality Upda..	449916503	Pat
KB4503290: Wind..	125818	CVE-2019-0..	High	High	High	9.8	10	3/20/2021	06/11/2019	Windows	MS19-JUN: Security Only Quality Updat..	450329003	Pat
KB4507457:	126570	CVE-2019-0..	High	High	High	9	9	3/20/2021	07/09/2019	Windows	MS19-JUL: Security Only Quality Updat..	450745701	Pat

Detected Vulnerabilities without Available Fixlets





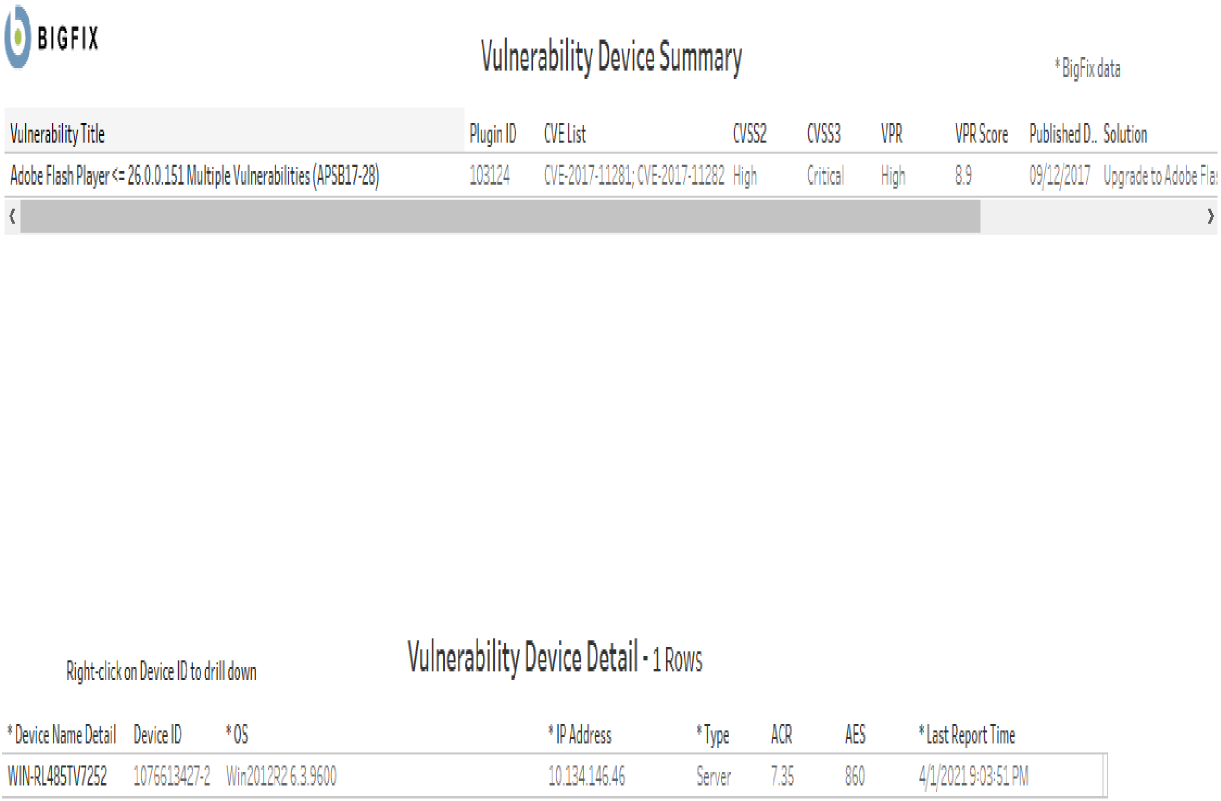
BIGFIX

Right-click on Plugin ID to drill down

* BigFix data

Vulnerability List - 107 Rows

Vulnerability Title	Plugin ID	Applicable Devices	CVE List	CVSS2	CVSS3	VPR	VPR
Adobe Flash Player <= 23.0.0.207 Multiple Vulnerabilities (APSB16-39)	95762	1	CVE-2016-7867; CVE-2016-7868; CVE-2016-7869; CVE-2016-7870; C..	High	Critical	High	8.9
Adobe Flash Player <= 24.0.0.186 Multiple Vulnerabilities (APSB17-02)	96388	1	CVE-2017-2925; CVE-2017-2926; CVE-2017-2927; CVE-2017-2928; C..	High	Critical	High	8.9
Adobe Flash Player <= 24.0.0.194 Multiple Vulnerabilities (APSB17-04)	97142	1	CVE-2017-2982; CVE-2017-2984; CVE-2017-2985; CVE-2017-2986; C..	High	Critical	High	8.9
Adobe Flash Player <= 25.0.0.127 Multiple Vulnerabilities (APSB17-10)	99283	1	CVE-2017-3058; CVE-2017-3059; CVE-2017-3060; CVE-2017-3061; C..	High	Critical	High	7.4
Adobe Flash Player <= 25.0.0.148 Multiple Vulnerabilities (APSB17-15)	100052	1	CVE-2017-3068; CVE-2017-3069; CVE-2017-3070; CVE-2017-3071; C..	High	Critical	High	8.9
Adobe Flash Player <= 25.0.0.171 Multiple Vulnerabilities (APSB17-17)	100756	1	CVE-2017-3075; CVE-2017-3076; CVE-2017-3077; CVE-2017-3078; C..	High	Critical	High	8.9
Adobe Flash Player <= 26.0.0.131 Multiple Vulnerabilities (APSB17-21)	101362	1	CVE-2017-3080; CVE-2017-3099; CVE-2017-3100	High	Critical	High	8.9
Adobe Flash Player <= 26.0.0.137 Multiple Vulnerabilities (APSB17-23)	102262	1	CVE-2017-3085; CVE-2017-3106	High	High	Medium	6.7
Adobe Flash Player <= 26.0.0.151 Multiple Vulnerabilities (APSB17-28)	103124	1	CVE-2017-11281; CVE-2017-11282	High	Critical	High	8.9
Adobe Flash Player <= 27.0.0.183 (APSB17-33)	104544	1	CVE-2017-11213; CVE-2017-11215; CVE-2017-11225; CVE-2017-311..	High	Critical	Medium	6.7
Adobe Flash Player <= 28.0.0.137 Use-after-free Remote Code Execution (A..	106606	1	CVE-2018-4877; CVE-2018-4878	High	Critical	High	9.6
Adobe Flash Player <= 28.0.0.161 (APSB18-05)	108281	1	CVE-2018-4919; CVE-2018-4920	High	Critical	Medium	6.7
Adobe Flash Player <= 29.0.0.113 (APSB18-08)	108958	1	CVE-2018-4932; CVE-2018-4933; CVE-2018-4934; CVE-2018-4935; C..	High	Critical	High	8.9
Adobe Flash Player <= 29.0.0.171 (APSB18-19)	110397	1	CVE-2018-4945; CVE-2018-5000; CVE-2018-5001; CVE-2018-5002	High	Critical	High	9.2
Adobe Flash Player <= 30.0.0.134 (APSB18-25)	111683	2	CVE-2018-12824; CVE-2018-12825; CVE-2018-12826; CVE-2018-12827; CVE-2018-12828	High	Critical	Medium	6.7
Adobe Flash Player <= 31.0.0.148 (APSB18-44)	119094	3	CVE-2018-15981	High	Critical	Medium	5.9
Adobe Flash Player <= 31.0.0.153 (APSB18-42)	119462	3	CVE-2018-15982; CVE-2018-15983	High	Critical	High	9.7
Adobe Flash Player <= 32.0.0.156 (APSB19-19)	123938	3	CVE-2019-7096; CVE-2019-7108	High	Critical	Medium	5.9
Adobe Flash Player Unsupported Version Detection	59196	3	Null	High		N/A	0
KB4018483: Security update for Adobe Flash Player (April 2017)	99290	1	CVE-2017-3058; CVE-2017-3059; CVE-2017-3060; CVE-2017-3061; C..	High	Critical	High	7.4
KB4020821: Security update for Adobe Flash Player (May 2017)	100062	1	CVE-2017-3068; CVE-2017-3069; CVE-2017-3070; CVE-2017-3071; C	High	Critical	High	8.9



Vulnerability Device Summary

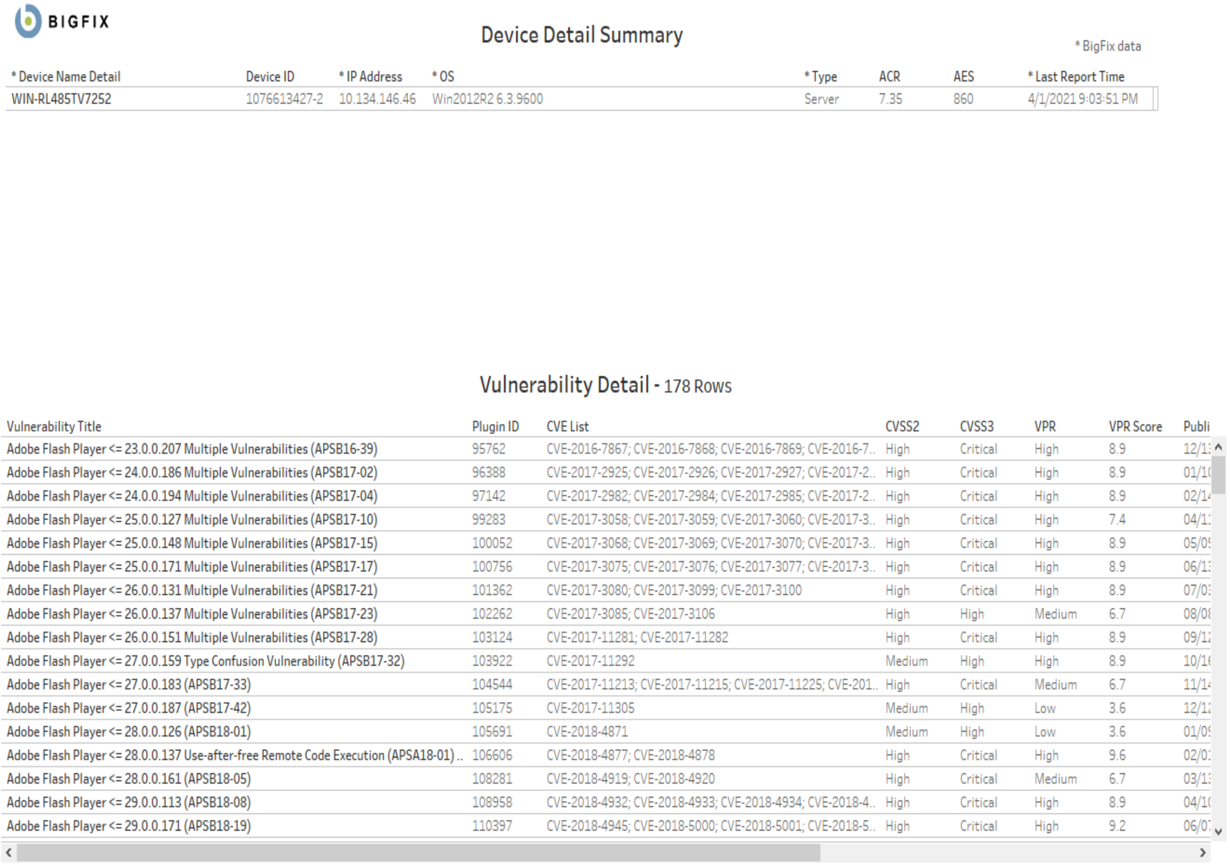
* BigFix data

Vulnerability Title	Plugin ID	CVE List	CVSS2	CVSS3	VPR	VPR Score	Published D..	Solution
Adobe Flash Player <= 26.0.0.151 Multiple Vulnerabilities (APSB17-28)	103124	CVE-2017-11281; CVE-2017-11282	High	Critical	High	8.9	09/12/2017	Upgrade to Adobe Fla:

Right-click on Device ID to drill down

Vulnerability Device Detail - 1 Rows

* Device Name Detail	Device ID	* OS	* IP Address	* Type	ACR	AES	* Last Report Time
WIN-RL485TV7252	1076613427-2	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM



Device Detail Summary

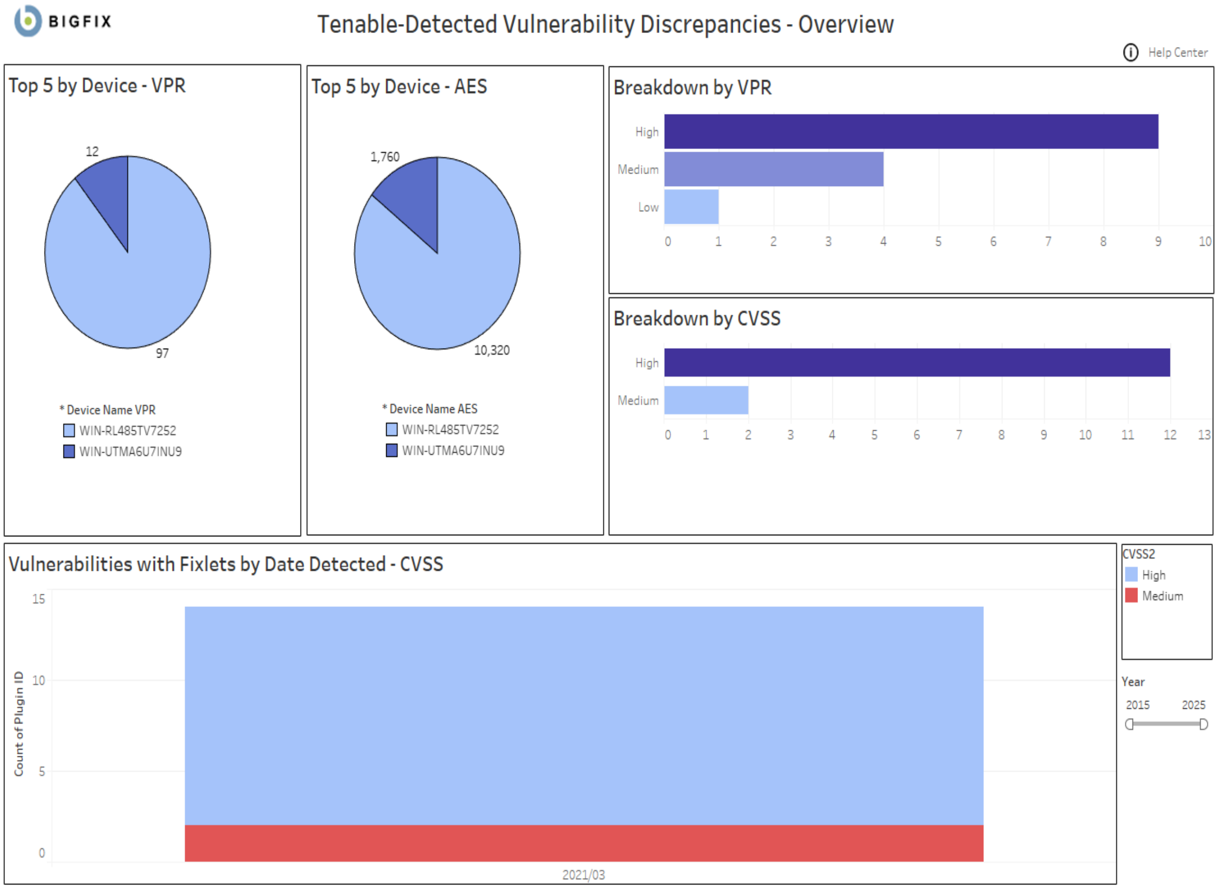
* BigFix data

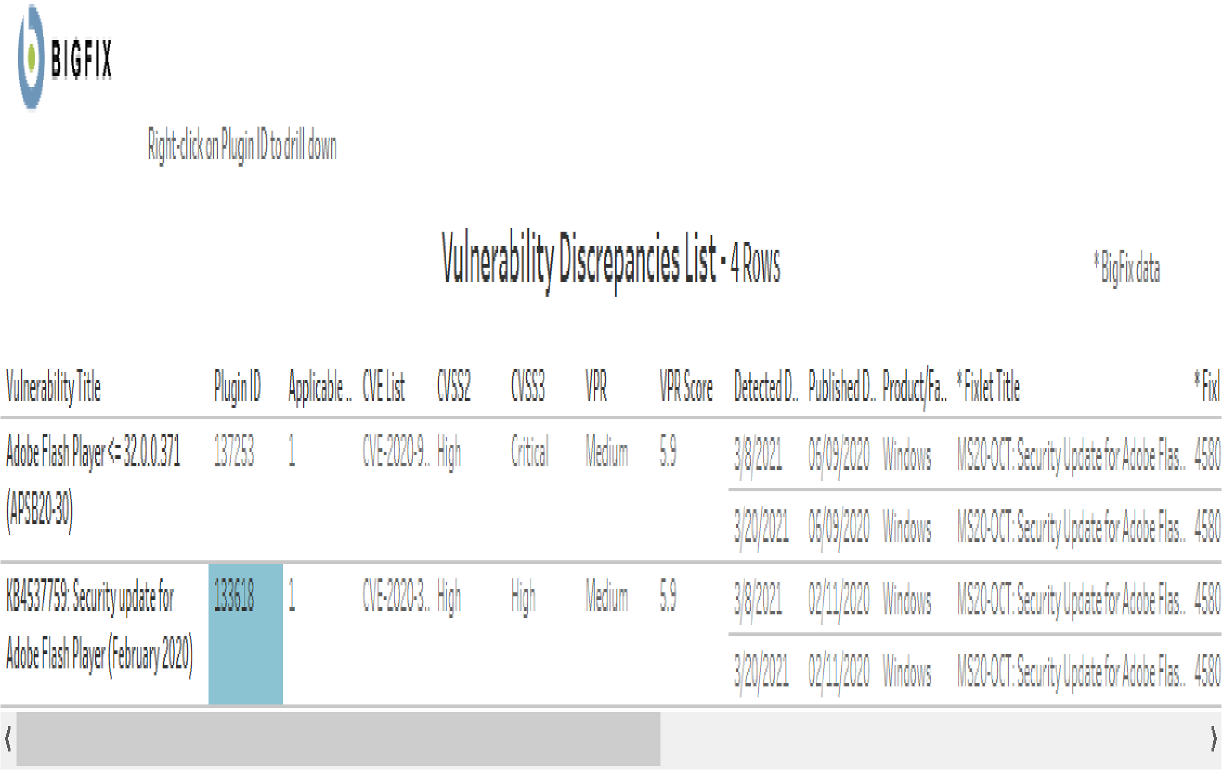
* Device Name Detail	Device ID	* IP Address	* OS	* Type	ACR	AES	* Last Report Time
WIN-RL485TV7252	1076613427-2	10.134.146.46	Win2012R2 6.3.9600	Server	7.35	860	4/1/2021 9:03:51 PM

Vulnerability Detail - 178 Rows

Vulnerability Title	Plugin ID	CVE List	CVSS2	CVSS3	VPR	VPR Score	Publi
Adobe Flash Player <= 23.0.0.207 Multiple Vulnerabilities (APSB16-39)	95762	CVE-2016-7867; CVE-2016-7868; CVE-2016-7869; CVE-2016-7..	High	Critical	High	8.9	12/1
Adobe Flash Player <= 24.0.0.186 Multiple Vulnerabilities (APSB17-02)	96388	CVE-2017-2925; CVE-2017-2926; CVE-2017-2927; CVE-2017-2..	High	Critical	High	8.9	01/1
Adobe Flash Player <= 24.0.0.194 Multiple Vulnerabilities (APSB17-04)	97142	CVE-2017-2982; CVE-2017-2984; CVE-2017-2985; CVE-2017-2..	High	Critical	High	8.9	02/1
Adobe Flash Player <= 25.0.0.127 Multiple Vulnerabilities (APSB17-10)	99283	CVE-2017-3058; CVE-2017-3059; CVE-2017-3060; CVE-2017-3..	High	Critical	High	7.4	04/1
Adobe Flash Player <= 25.0.0.148 Multiple Vulnerabilities (APSB17-15)	100052	CVE-2017-3068; CVE-2017-3069; CVE-2017-3070; CVE-2017-3..	High	Critical	High	8.9	05/0
Adobe Flash Player <= 25.0.0.171 Multiple Vulnerabilities (APSB17-17)	100756	CVE-2017-3075; CVE-2017-3076; CVE-2017-3077; CVE-2017-3..	High	Critical	High	8.9	06/1
Adobe Flash Player <= 26.0.0.131 Multiple Vulnerabilities (APSB17-21)	101362	CVE-2017-3080; CVE-2017-3099; CVE-2017-3100	High	Critical	High	8.9	07/0
Adobe Flash Player <= 26.0.0.137 Multiple Vulnerabilities (APSB17-23)	102262	CVE-2017-3085; CVE-2017-3106	High	High	Medium	6.7	08/0
Adobe Flash Player <= 26.0.0.151 Multiple Vulnerabilities (APSB17-28)	103124	CVE-2017-11281; CVE-2017-11282	High	Critical	High	8.9	09/1
Adobe Flash Player <= 27.0.0.159 Type Confusion Vulnerability (APSB17-32)	103922	CVE-2017-11292	Medium	High	High	8.9	10/1
Adobe Flash Player <= 27.0.0.183 (APSB17-33)	104544	CVE-2017-11213; CVE-2017-11215; CVE-2017-11225; CVE-201..	High	Critical	Medium	6.7	11/1
Adobe Flash Player <= 27.0.0.187 (APSB17-42)	105175	CVE-2017-11305	Medium	High	Low	3.6	12/1
Adobe Flash Player <= 28.0.0.126 (APSB18-01)	105691	CVE-2018-4871	Medium	High	Low	3.6	01/0
Adobe Flash Player <= 28.0.0.137 Use-after-free Remote Code Execution (APSA18-01) ..	106606	CVE-2018-4877; CVE-2018-4878	High	Critical	High	9.6	02/0
Adobe Flash Player <= 28.0.0.161 (APSB18-05)	108281	CVE-2018-4919; CVE-2018-4920	High	Critical	Medium	6.7	03/1
Adobe Flash Player <= 29.0.0.113 (APSB18-08)	108958	CVE-2018-4932; CVE-2018-4933; CVE-2018-4934; CVE-2018-4..	High	Critical	High	8.9	04/1
Adobe Flash Player <= 29.0.0.171 (APSB18-19)	110397	CVE-2018-4945; CVE-2018-5000; CVE-2018-5001; CVE-2018-5..	High	Critical	High	9.2	06/0

Vulnerability Discrepancies



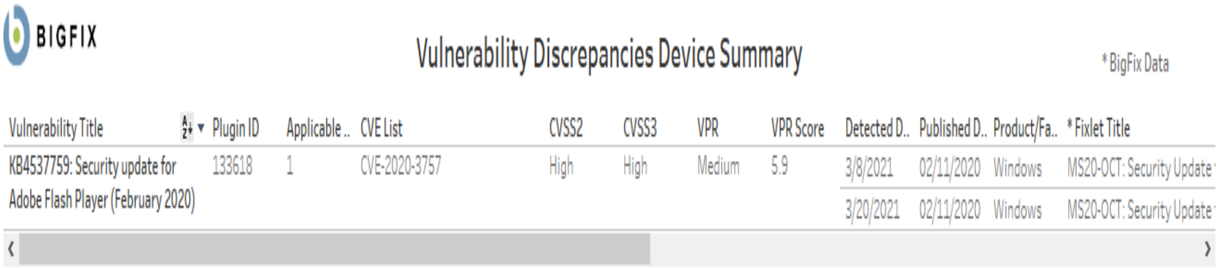


Right-click on Plugin ID to drill down

Vulnerability Discrepancies List - 4 Rows

*BigFix data

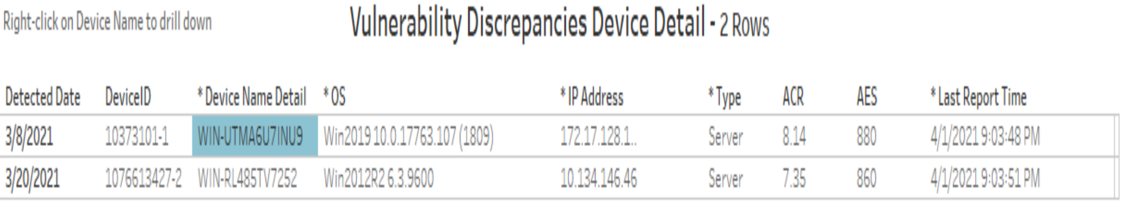
Vulnerability Title	Plugin ID	Applicable ..	CVE List	CVSS2	CVSS3	VPR	VPR Score	Detected D..	Published D..	Product/Fa..	*Fixlet Title	*Fixl
Adobe Flash Player <= 32.0.0.371 (APSB20-30)	137253	1	CVE-2020-9..	High	Critical	Medium	5.9	3/8/2021	06/09/2020	Windows	MS20-OCT: Security Update for Adobe Flas..	4580
								3/20/2021	06/09/2020	Windows	MS20-OCT: Security Update for Adobe Flas..	4580
KB4537759: Security update for Adobe Flash Player (February 2020)	133618	1	CVE-2020-3..	High	High	Medium	5.9	3/8/2021	02/11/2020	Windows	MS20-OCT: Security Update for Adobe Flas..	4580
								3/20/2021	02/11/2020	Windows	MS20-OCT: Security Update for Adobe Flas..	4580



Vulnerability Discrepancies Device Summary

*BigFix Data

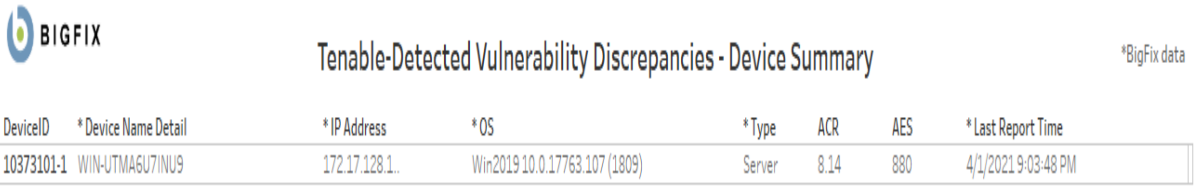
Vulnerability Title	Plugin ID	Applicable ..	CVE List	CVSS2	CVSS3	VPR	VPR Score	Detected D..	Published D..	Product/Fa..	* Fixlet Title
KB4537759: Security update for Adobe Flash Player (February 2020)	133618	1	CVE-2020-3757	High	High	Medium	5.9	3/8/2021	02/11/2020	Windows	MS20-OCT: Security Update
								3/20/2021	02/11/2020	Windows	MS20-OCT: Security Update



Right-click on Device Name to drill down

Vulnerability Discrepancies Device Detail - 2 Rows

Detected Date	DeviceID	* Device Name Detail	* OS	* IP Address	* Type	ACR	AES	* Last Report Time
3/8/2021	10373101-1	WIN-UTMA6U7INU9	Win2019 10.0.17763.107 (1809)	172.17.128.1..	Server	8.14	880	4/1/2021 9:03:48 PM
3/20/2021	1076613427-2	WIN-RL485TV7252	Win2012R2 6.3.9600	10.134.146.46	Server	7.35	860	4/1/2021 9:03:51 PM

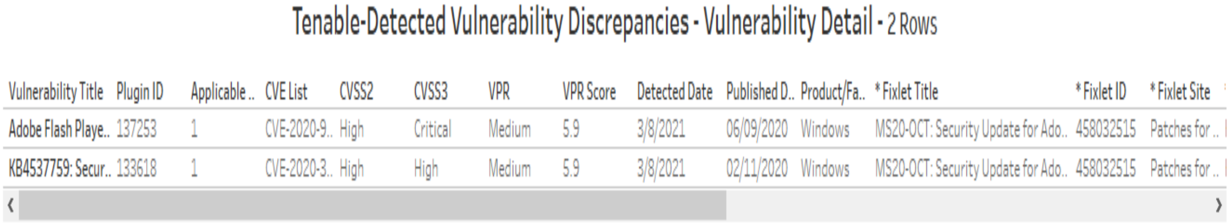


BIGFIX

Tenable-Detected Vulnerability Discrepancies - Device Summary

*BigFix data

DeviceID	* Device Name Detail	* IP Address	* OS	* Type	ACR	AES	* Last Report Time
10373101-1	WIN-UTMA6U7INU9	172.17.128.1..	Win2019 10.0.17763.107 (1809)	Server	8.14	880	4/1/2021 9:03:48 PM



Tenable-Detected Vulnerability Discrepancies - Vulnerability Detail - 2 Rows

Vulnerability Title	Plugin ID	Applicable ..	CVE List	CVSS2	CVSS3	VPR	VPR Score	Detected Date	Published D..	Product/Fa..	* Fixlet Title	* Fixlet ID	* Fixlet Site
Adobe Flash Playe..	137253	1	CVE-2020-9..	High	Critical	Medium	5.9	3/8/2021	06/09/2020	Windows	MS20-OCT: Security Update for Ado..	458032515	Patches for ..
KB4537759: Secur..	133618	1	CVE-2020-3..	High	High	Medium	5.9	3/8/2021	02/11/2020	Windows	MS20-OCT: Security Update for Ado..	458032515	Patches for ..

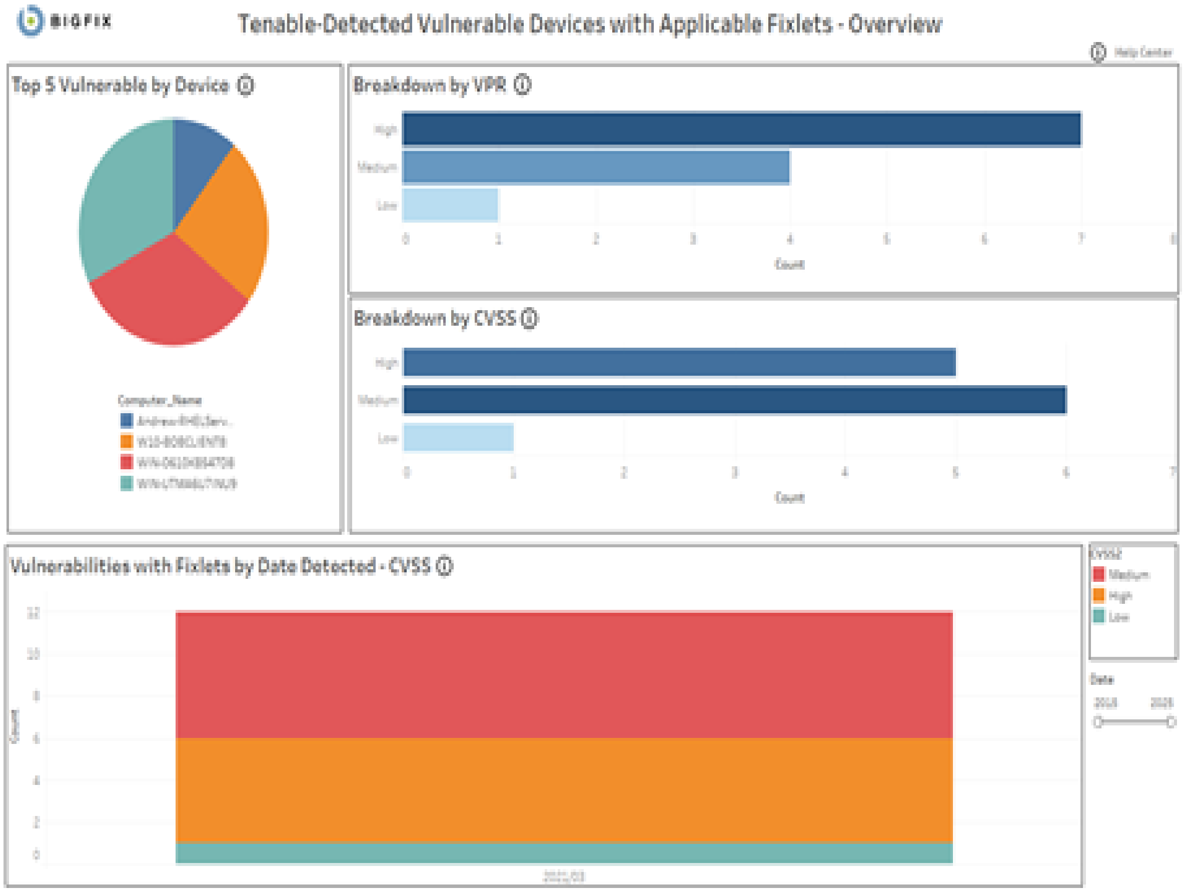
Tableau reports for Tenable.sc

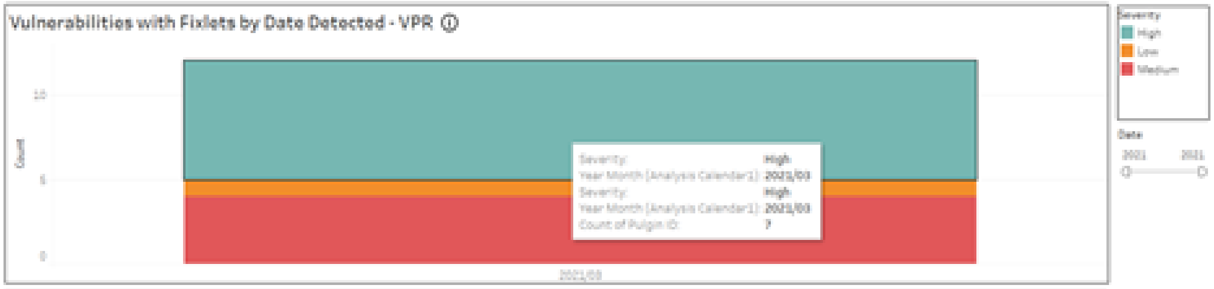
Use this section to become familiar with Tableau reports for Tenable.sc

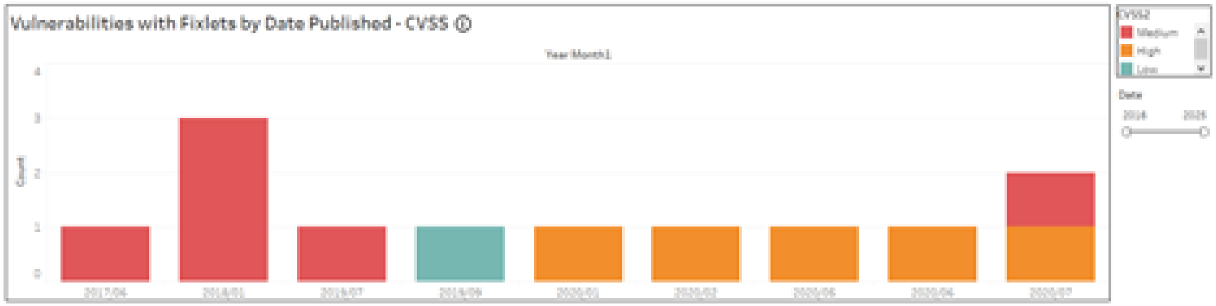
Chart details:

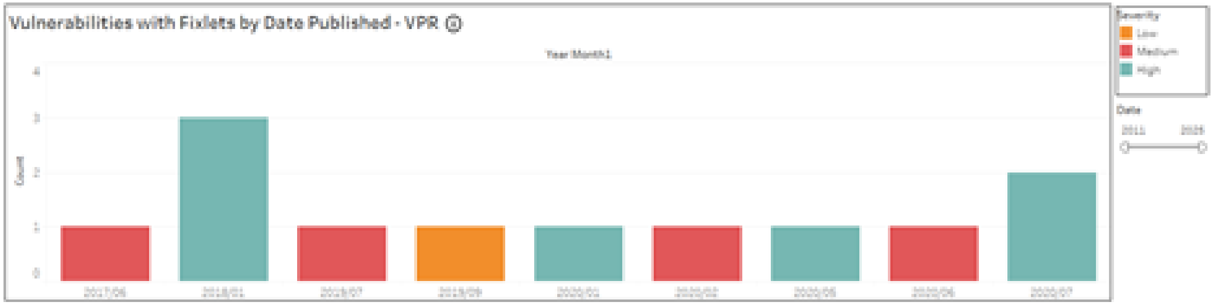
- Vulnerability Title - Vulnerability title
- PluginID - a unique identifier assigned to a vulnerability detection
- Applicable Devices - devices that have been scanned by Tenable and for which vulnerabilities have been identified
- CVE List - list of CVE
- CVSS2 - (Common Vulnerability Scoring System version 2), scoring system used to assess the severity and potential impact of security vulnerabilities.
- CVSS3 - (Common Vulnerability Scoring System version 3), updated version of the scoring system
- VPR - Vulnerability Priority Rating
- VPR Score - numerical value ranging from 0 to 10, with 10 being the highest priority
- Detected Date - the date when a vulnerability was first detected
- Published Date - date when the information about a vulnerability was first available

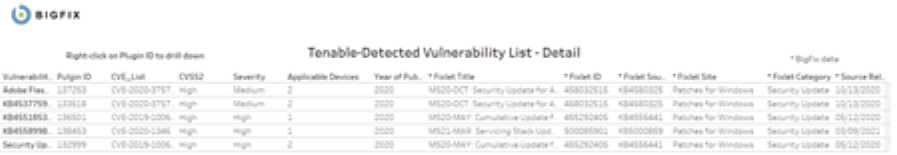
Detected Vulnerabilities with Applicable Fixlets











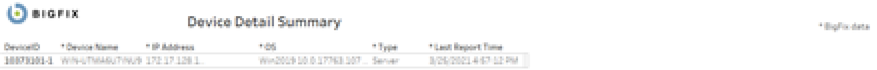
BIGFIX

Right-click on Plugin ID to drill down

Tenable-Detected Vulnerability List - Detail

* BigFix data

Vulnerabilit..	Pulgin ID	CVE_List	CVSS2	Severity	Applicable Devices	Year of Pub..	* Fixlet Title	* Fixlet ID	* Fixlet Sou..	* Fixlet Site	* Fixlet Category	* Source Rel..
Adobe Flas..	137253	CVE-2020-3757..	High	Medium	2	2020	MS20-OCT: Security Update for A..	458032515	KB4580325	Patches for Windows	Security Update	10/13/2020
KB4537759..	133618	CVE-2020-3757..	High	Medium	2	2020	MS20-OCT: Security Update for A..	458032515	KB4580325	Patches for Windows	Security Update	10/13/2020
KB4551853..	136501	CVE-2019-1006..	High	High	1	2020	MS20-MAY: Cumulative Update f..	455292405	KB4556441	Patches for Windows	Security Update	05/12/2020
KB4558998..	138453	CVE-2020-1346..	High	High	1	2020	MS21-MAR: Servicing Stack Upd..	500085901	KB5000859	Patches for Windows	Security Update	03/09/2021
Security Up..	132999	CVE-2019-1006..	High	High	2	2020	MS20-MAY: Cumulative Update f..	455292405	KB4556441	Patches for Windows	Security Update	05/12/2020

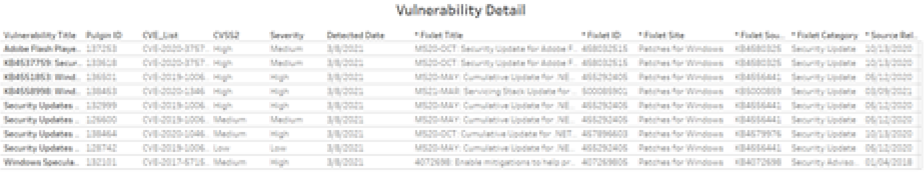


BIGFIX

Device Detail Summary

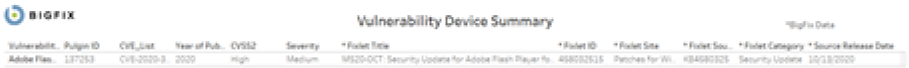
* BigFix data

DeviceID	* Device Name	* IP Address	* OS	* Type	* Last Report Time
10073101-1	WIN-UTMA6UTVNU9	172.17.128.1..	Win2019 10.0.17763.107..	Server	3/26/2021 4:57:12 PM



Vulnerability Detail

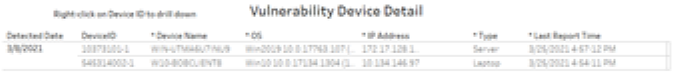
Vulnerability Title	Pulgin ID	CVE_List	CVSS2	Severity	Detected Date	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Rel..
Adobe Flash Playe..	137253	CVE-2020-3757..	High	Medium	3/8/2021	MS20-OCT: Security Update for Adobe F..	458032515	Patches for Windows	KB4580325	Security Update	10/13/2020
KB4537759: Secur..	133618	CVE-2020-3757..	High	Medium	3/8/2021	MS20-OCT: Security Update for Adobe F..	458032515	Patches for Windows	KB4580325	Security Update	10/13/2020
KB4551853: Wind..	136501	CVE-2019-1006..	High	High	3/8/2021	MS20-MAY: Cumulative Update for .NE..	455292405	Patches for Windows	KB4556441	Security Update	05/12/2020
KB4558998: Wind..	138453	CVE-2020-1346..	High	High	3/8/2021	MS21-MAR: Servicing Stack Update for ..	500085901	Patches for Windows	KB5000859	Security Update	03/09/2021
Security Updates ..	132999	CVE-2019-1006..	High	High	3/8/2021	MS20-MAY: Cumulative Update for .NE..	455292405	Patches for Windows	KB4556441	Security Update	05/12/2020
Security Updates ..	126600	CVE-2019-1006..	Medium	Medium	3/8/2021	MS20-MAY: Cumulative Update for .NE..	455292405	Patches for Windows	KB4556441	Security Update	05/12/2020
Security Updates ..	138464	CVE-2020-1046..	Medium	High	3/8/2021	MS20-OCT: Cumulative Update for .NET..	457899603	Patches for Windows	KB4579976	Security Update	10/13/2020
Security Updates ..	128742	CVE-2019-1006..	Low	Low	3/8/2021	MS20-MAY: Cumulative Update for .NE..	455292405	Patches for Windows	KB4556441	Security Update	05/12/2020
Windows Specula..	132101	CVE-2017-5715..	Medium	High	3/8/2021	4072698: Enable mitigations to help pr..	407269805	Patches for Windows	KB4072698	Security Adviso..	01/04/2018



Vulnerability Device Summary

*BigFix Data

Vulnerabilit..	Pulgin ID	CVE_List	Year of Pub..	CVSS2	Severity	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Release Date
Adobe Flas..	137253	CVE-2020-3..	2020	High	Medium	MS20-OCT: Security Update for Adobe Flash Player fo..	458032515	Patches for Wi..	KB4580325	Security Update	10/13/2020

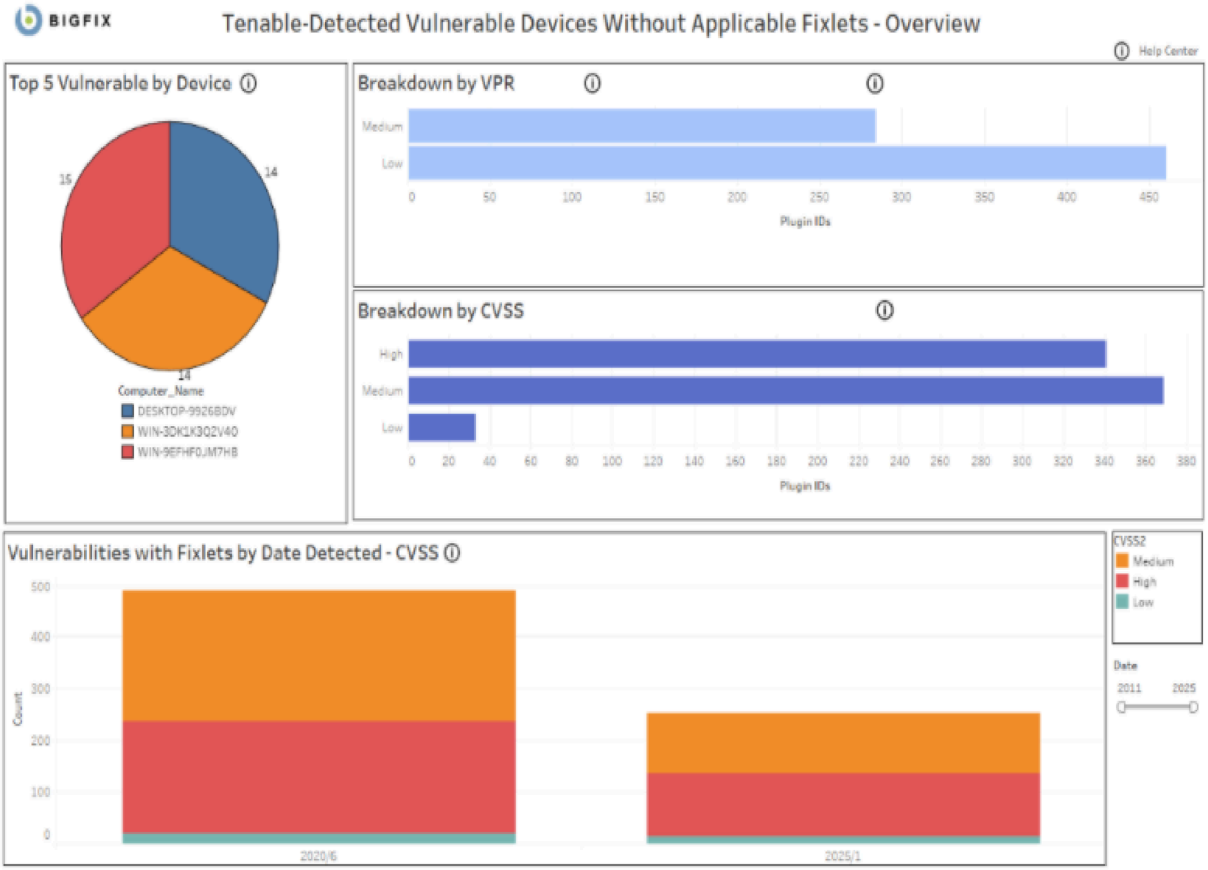


Right-click on Device ID to drill down

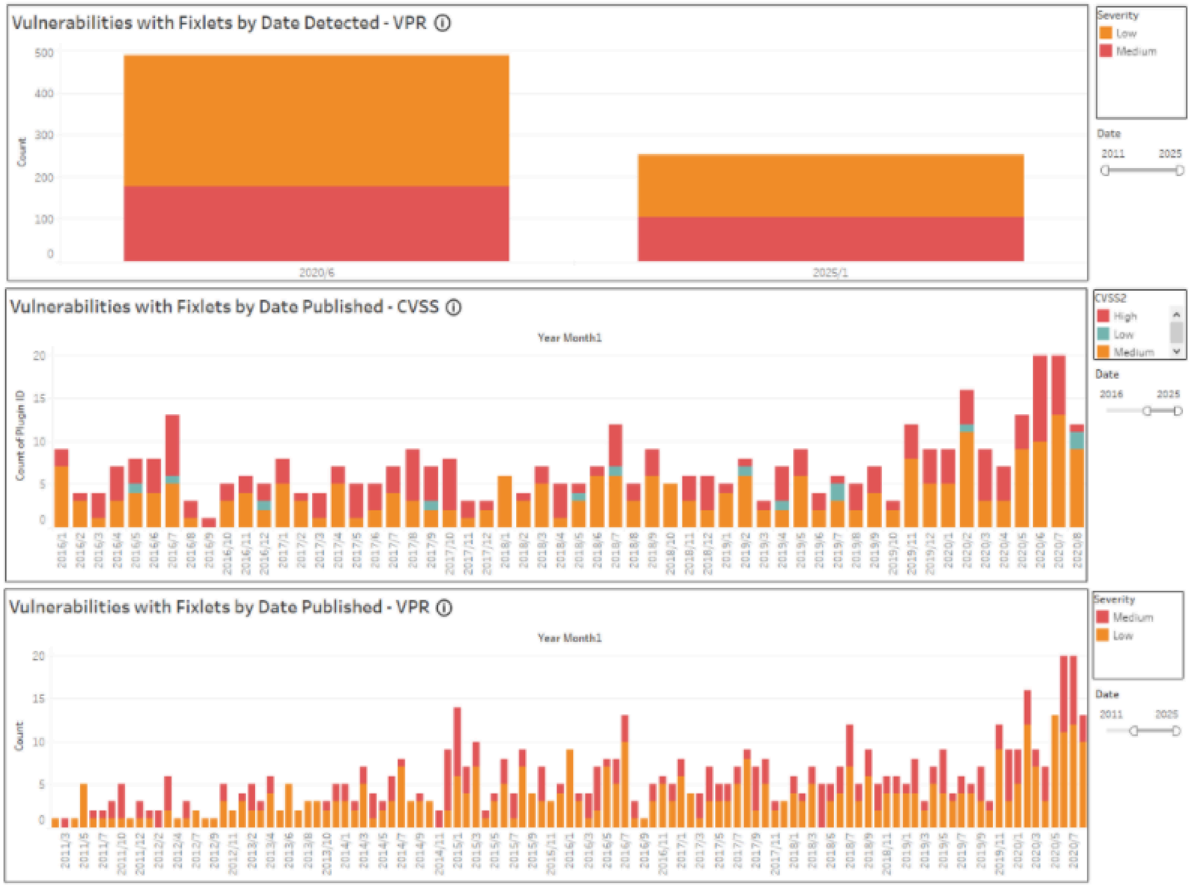
Vulnerability Device Detail

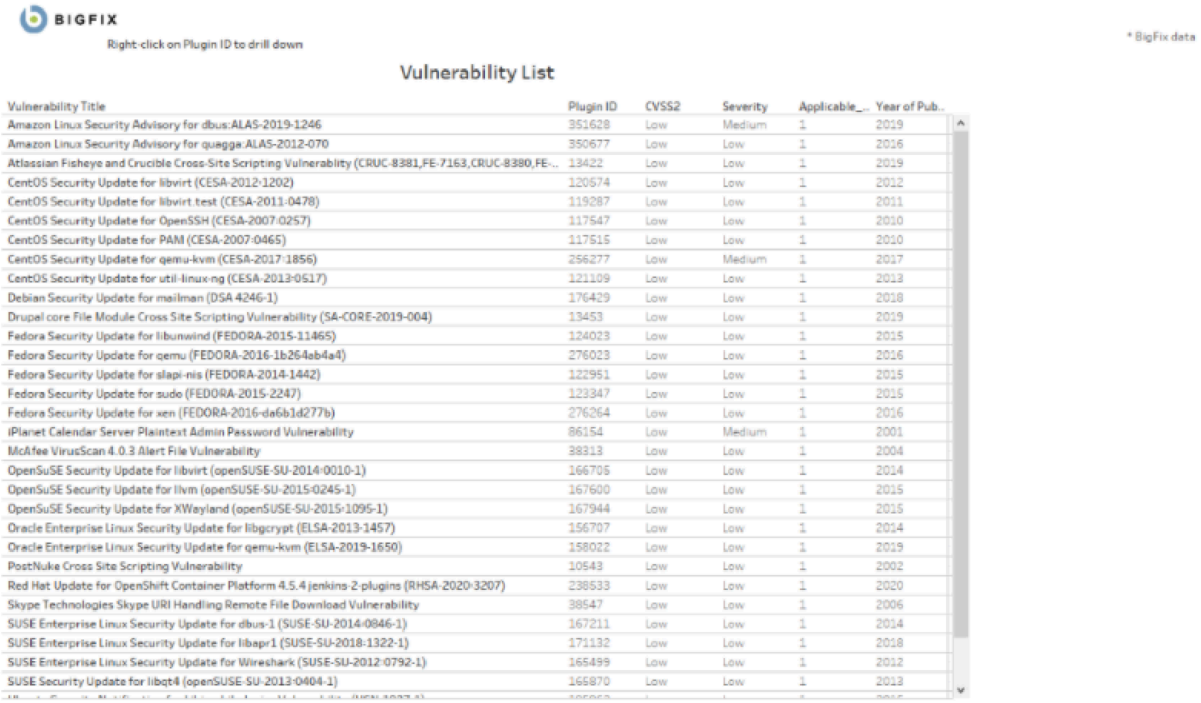
Detected Date	DeviceID	* Device Name	* OS	* IP Address	* Type	* Last Report Time
3/8/2021	10373101-1	WIN-UTM46UT/NU9	Win2019 10.0.17763.107 (..	172.17.128.1..	Server	3/25/2021 4:57:12 PM
	545314002-1	W10-8O8CU/ENT8	Win10 10.0.17134.1304 (1..	10.134.146.97	Laptop	3/25/2021 4:54:11 PM

Detected Vulnerabilities without Available Fixlets



Tenable-Detected Vulnerable Devices Without Applicable Fixlets - Overview



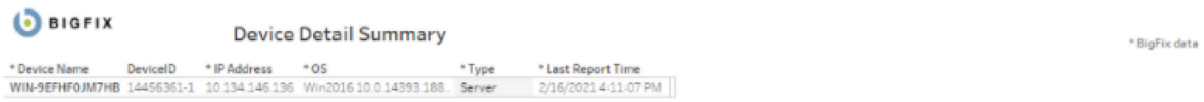


Right-click on Plugin ID to drill down

* BigFix data

Vulnerability List

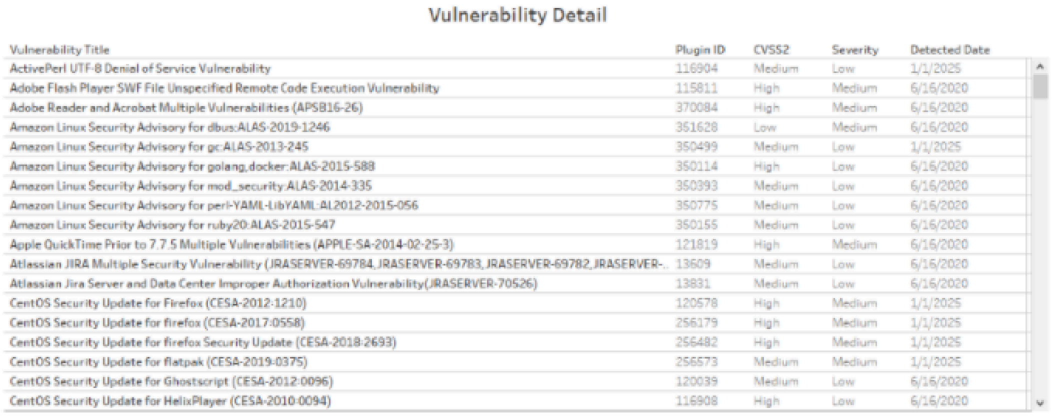
Vulnerability Title	Plugin ID	CVSS2	Severity	Applicable_..	Year of Pub..
Amazon Linux Security Advisory for dbus:ALAS-2019-1246	351628	Low	Medium	1	2019
Amazon Linux Security Advisory for quagga:ALAS-2012-070	350677	Low	Low	1	2016
Atlassian Fisheye and Crucible Cross-Site Scripting Vulnerablity (CRUC-8381,FE-7163,CRUC-8380,FE-..	13422	Low	Low	1	2019
CentOS Security Update for libvirt (CESA-2012:1202)	120574	Low	Low	1	2012
CentOS Security Update for libvirt.test (CESA-2011:0478)	119287	Low	Low	1	2011
CentOS Security Update for OpenSSH (CESA-2007:0257)	117547	Low	Low	1	2010
CentOS Security Update for PAM (CESA-2007:0465)	117515	Low	Low	1	2010
CentOS Security Update for qemu-kvm (CESA-2017:1856)	256277	Low	Medium	1	2017
CentOS Security Update for util-linux-ng (CESA-2013:0517)	121109	Low	Low	1	2013
Debian Security Update for mailman (DSA 4246-1)	176429	Low	Low	1	2018
Drupal core File Module Cross Site Scripting Vulnerability (SA-CORE-2019-004)	13453	Low	Low	1	2019
Fedora Security Update for libunwind (FEDORA-2015-11465)	124023	Low	Low	1	2015
Fedora Security Update for qemu (FEDORA-2016-1b264ab4a4)	276023	Low	Low	1	2016
Fedora Security Update for slapi-nis (FEDORA-2014-1442)	122951	Low	Low	1	2015
Fedora Security Update for sudo (FEDORA-2015-2247)	123347	Low	Low	1	2015
Fedora Security Update for xen (FEDORA-2016-da6b1d277b)	276264	Low	Low	1	2016
iPlanet Calendar Server Plaintext Admin Password Vulnerability	86154	Low	Medium	1	2001
McAfee VirusScan 4.0.3 Alert File Vulnerability	38313	Low	Low	1	2004
OpenSuSE Security Update for libvirt (openSUSE-SU-2014:0010-1)	166705	Low	Low	1	2014
OpenSuSE Security Update for llvm (openSUSE-SU-2015:0245-1)	167600	Low	Low	1	2015
OpenSuSE Security Update for XWayland (openSUSE-SU-2015:1095-1)	167944	Low	Low	1	2015
Oracle Enterprise Linux Security Update for libgcrypt (ELSA-2013-1457)	156707	Low	Low	1	2014
Oracle Enterprise Linux Security Update for qemu-kvm (ELSA-2019-1650)	158022	Low	Low	1	2019
PostNuke Cross Site Scripting Vulnerability	10543	Low	Low	1	2002
Red Hat Update for OpenShift Container Platform 4.5.4 jenkins-2-plugins (RHSA-2020:3207)	238533	Low	Low	1	2020
Skype Technologies Skype URI Handling Remote File Download Vulnerability	38547	Low	Low	1	2006
SUSE Enterprise Linux Security Update for dbus-1 (SUSE-SU-2014:0846-1)	167211	Low	Low	1	2014
SUSE Enterprise Linux Security Update for libapr1 (SUSE-SU-2018:1322-1)	171132	Low	Low	1	2018
SUSE Enterprise Linux Security Update for Wireshark (SUSE-SU-2012:0792-1)	165499	Low	Low	1	2012
SUSE Security Update for libqt4 (openSUSE-SU-2013:0404-1)	165870	Low	Low	1	2013



Device Detail Summary

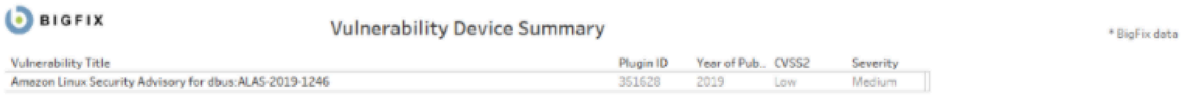
* BigFix data

* Device Name	DeviceID	* IP Address	* OS	* Type	* Last Report Time
WIN-9EFHF0JM7HB	14456361-1	10.134.146.136	Win2016 10.0.14393.188..	Server	2/16/2021 4:11:07 PM



Vulnerability Detail

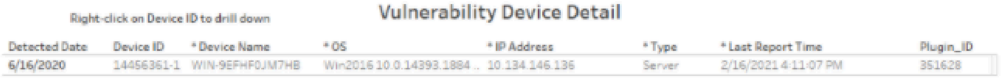
Vulnerability Title	Plugin ID	CVSS2	Severity	Detected Date
ActivePerl UTF-8 Denial of Service Vulnerability	116904	Medium	Low	1/1/2025
Adobe Flash Player SWF File Unspecified Remote Code Execution Vulnerability	115811	High	Medium	6/16/2020
Adobe Reader and Acrobat Multiple Vulnerabilities (APSB16-26)	370084	High	Medium	6/16/2020
Amazon Linux Security Advisory for dbus:ALAS-2019-1246	351628	Low	Medium	6/16/2020
Amazon Linux Security Advisory for gc:ALAS-2013-245	350499	Medium	Low	1/1/2025
Amazon Linux Security Advisory for golang,docker:ALAS-2015-588	350114	High	Low	6/16/2020
Amazon Linux Security Advisory for mod_security:ALAS-2014-335	350393	Medium	Low	6/16/2020
Amazon Linux Security Advisory for perl-YAML-LibYAML:AL2012-2015-056	350775	Medium	Low	6/16/2020
Amazon Linux Security Advisory for ruby20:ALAS-2015-547	350155	Medium	Low	6/16/2020
Apple QuickTime Prior to 7.7.5 Multiple Vulnerabilities (APPLE-SA-2014-02-25-3)	121819	High	Medium	6/16/2020
Atlassian JIRA Multiple Security Vulnerability (JRASERVER-69784, JRASERVER-69783, JRASERVER-69782, JRASERVER-..	13609	Medium	Low	6/16/2020
Atlassian Jira Server and Data Center Improper Authorization Vulnerability(JRASERVER-70526)	13831	Medium	Low	6/16/2020
CentOS Security Update for Firefox (CESA-2012:1210)	120578	High	Medium	1/1/2025
CentOS Security Update for firefox (CESA-2017:0558)	256179	High	Medium	1/1/2025
CentOS Security Update for firefox Security Update (CESA-2018:2693)	256482	High	Medium	1/1/2025
CentOS Security Update for flatpak (CESA-2019-0375)	256573	Medium	Medium	1/1/2025
CentOS Security Update for Ghostscript (CESA-2012:0096)	120039	Medium	Low	6/16/2020
CentOS Security Update for HelixPlayer (CESA-2010:0094)	116908	High	Low	6/16/2020



Vulnerability Device Summary

* BigFix data

Vulnerability Title	Plugin ID	Year of Pub..	CVSS2	Severity
Amazon Linux Security Advisory for dbus:ALAS-2019-1246	351628	2019	Low	Medium

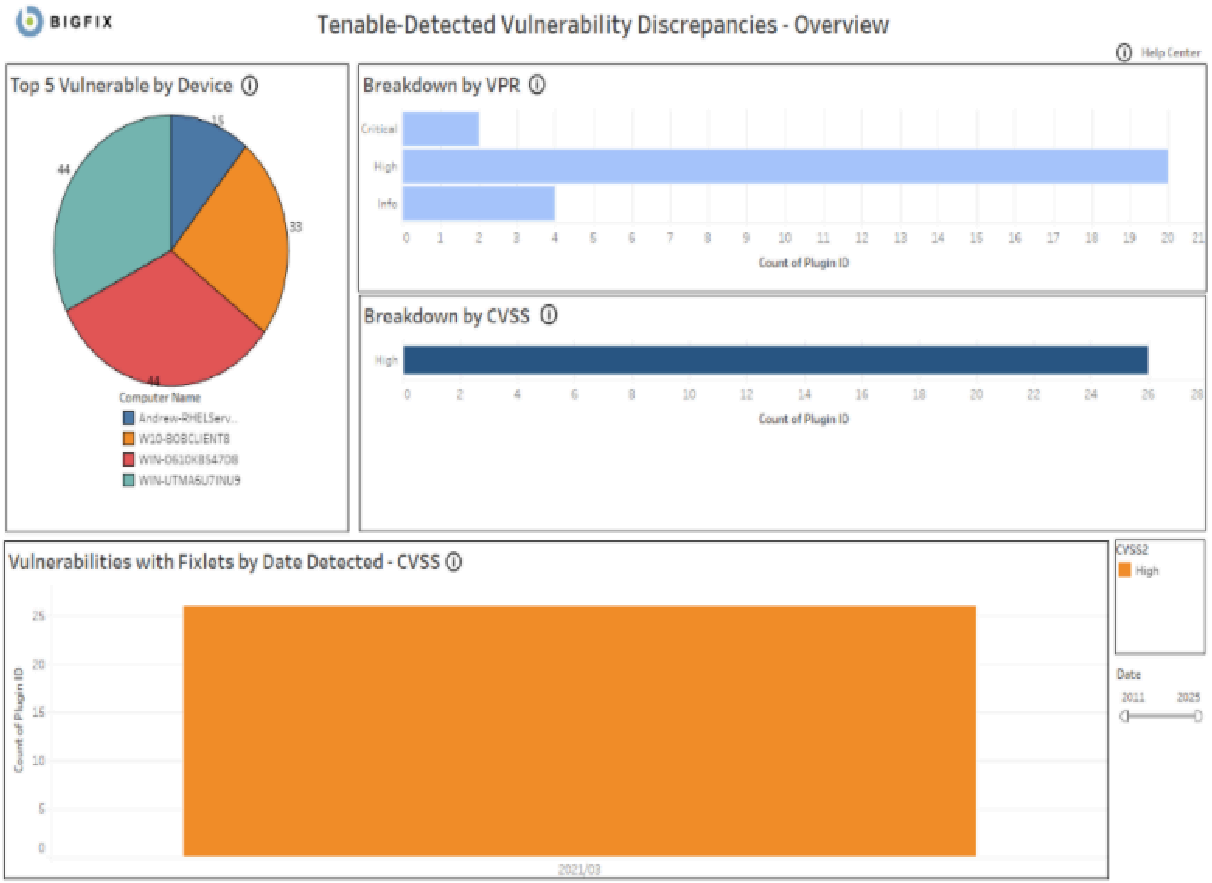


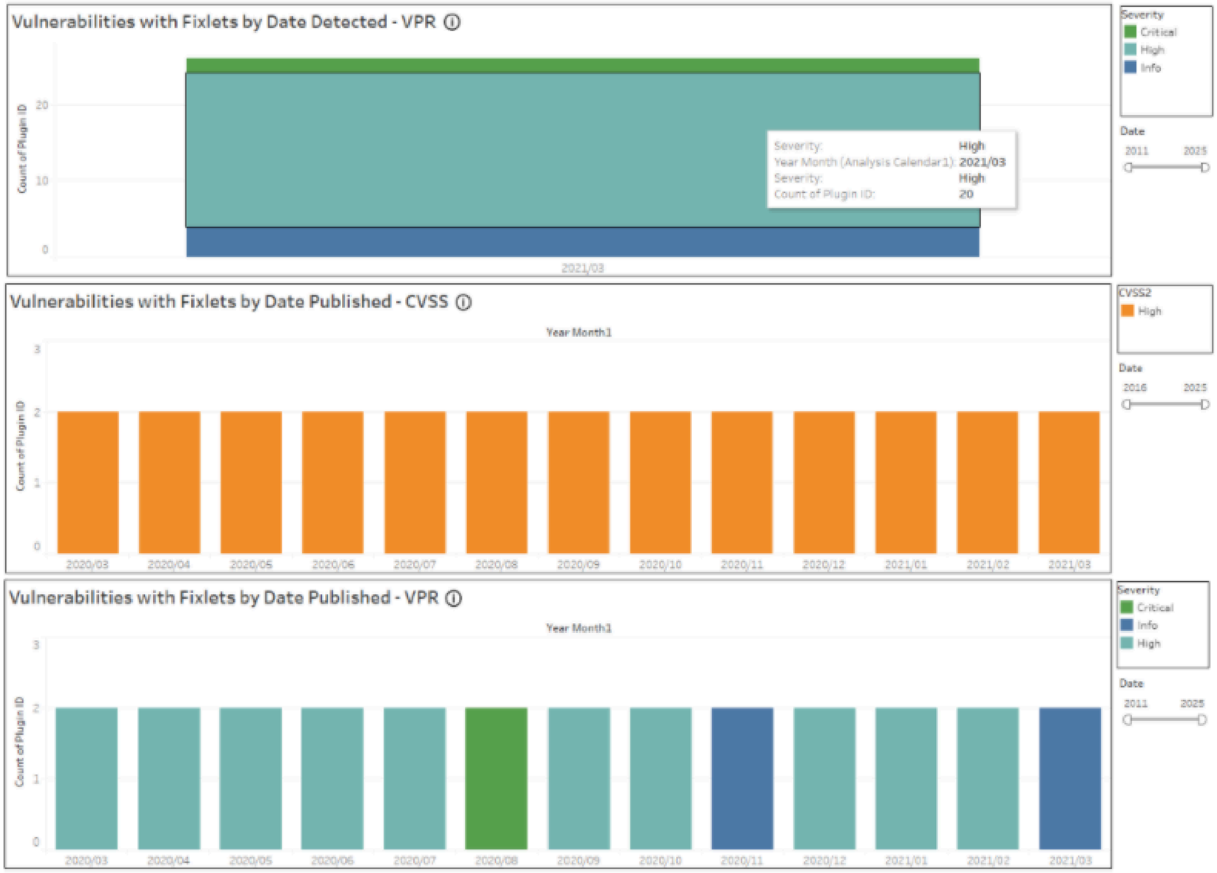
Right-click on Device ID to drill down

Vulnerability Device Detail

Detected Date	Device ID	* Device Name	* OS	* IP Address	* Type	* Last Report Time	Plugin_ID
6/16/2020	14456361-1	WIN-9EFHF0JM7HB	Win2016 10.0.14393.1884 ..	10.134.146.136	Server	2/16/2021 4:11:07 PM	351628

Vulnerability Discrepancies



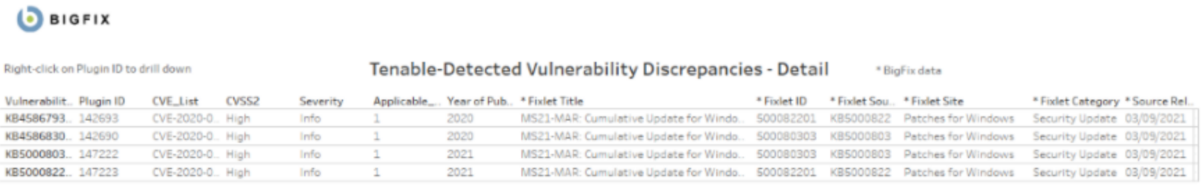


Vulnerabilities with Fixlets by Date Detected - VPR ⓘ

Severity: High
Year Month (Analysis Calendar1): 2021/03
Severity: High
Count of Plugin ID: 20

Vulnerabilities with Fixlets by Date Published - CVSS ⓘ

Vulnerabilities with Fixlets by Date Published - VPR ⓘ

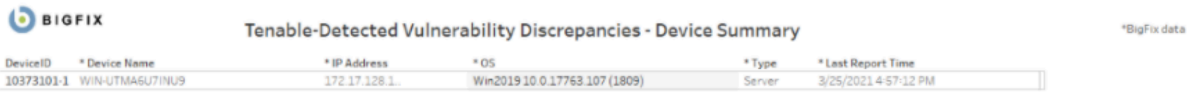


Right-click on Plugin ID to drill down

Tenable-Detected Vulnerability Discrepancies - Detail

* BigFix data

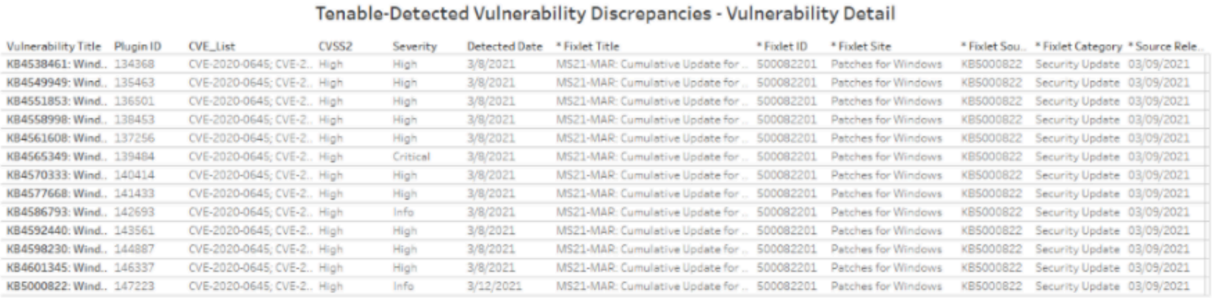
Vulnerabilit..	Plugin ID	CVE_List	CVSS2	Severity	Applicable_..	Year of Pub..	* Fixlet Title	* Fixlet ID	* Fixlet Sou..	* Fixlet Site	* Fixlet Category	* Source Rel..
KB4586793..	142693	CVE-2020-0..	High	Info	1	2020	MS21-MAR: Cumulative Update for Windo..	500082201	KB5000822	Patches for Windows	Security Update	03/09/2021
KB4586830..	142690	CVE-2020-0..	High	Info	1	2020	MS21-MAR: Cumulative Update for Windo..	500080303	KB5000803	Patches for Windows	Security Update	03/09/2021
KB5000803..	147222	CVE-2020-0..	High	Info	1	2021	MS21-MAR: Cumulative Update for Windo..	500080303	KB5000803	Patches for Windows	Security Update	03/09/2021
KB5000822..	147223	CVE-2020-0..	High	Info	1	2021	MS21-MAR: Cumulative Update for Windo..	500082201	KB5000822	Patches for Windows	Security Update	03/09/2021



Tenable-Detected Vulnerability Discrepancies - Device Summary

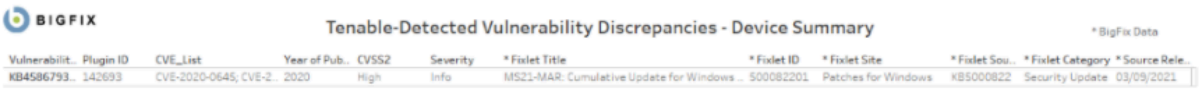
*BigFix data

DeviceID	* Device Name	* IP Address	* OS	* Type	* Last Report Time
10373101-1	WIN-UTMA6U7INU9	172.17.128.1..	Win2019 10.0.17763.107 (1809)	Server	3/25/2021 4:57:12 PM



Tenable-Detected Vulnerability Discrepancies - Vulnerability Detail

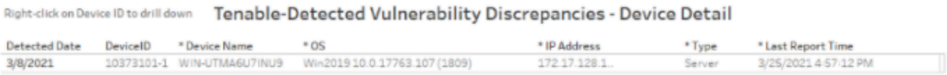
Vulnerability Title	Plugin ID	CVE_List	CVSS2	Severity	Detected Date	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Rele..
KB4538461: Wind..	134368	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4549949: Wind..	135463	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4551853: Wind..	136501	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4558998: Wind..	138453	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4561608: Wind..	137256	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4565349: Wind..	139484	CVE-2020-0645; CVE-2..	High	Critical	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4570333: Wind..	140414	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4577668: Wind..	141433	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4586793: Wind..	142693	CVE-2020-0645; CVE-2..	High	Info	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4592440: Wind..	143561	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4598230: Wind..	144887	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4601345: Wind..	146337	CVE-2020-0645; CVE-2..	High	High	3/8/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB5000822: Wind..	147223	CVE-2020-0645; CVE-2..	High	Info	3/12/2021	MS21-MAR: Cumulative Update for ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021



Tenable-Detected Vulnerability Discrepancies - Device Summary

* BigFix Data

Vulnerabilit..	Plugin ID	CVE_List	Year of Pub..	CVSS2	Severity	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou..	* Fixlet Category	* Source Rele..
KB4586793..	142693	CVE-2020-0645; CVE-2..	2020	High	Info	MS21-MAR: Cumulative Update for Windows ..	500082201	Patches for Windows	KB5000822	Security Update	03/09/2021



Right-click on Device ID to drill down

Tenable-Detected Vulnerability Discrepancies - Device Detail

Detected Date	DeviceID	* Device Name	* OS	* IP Address	* Type	* Last Report Time
3/8/2021	10373101-1	WIN-UTMA6U7INU9	Win2019 10.0.17763.107 (1809)	172.17.128.1..	Server	3/25/2021 4:57:12 PM

Chapter 10. Reference

The following topics contain information on how you can work with the configuration file and settings, the CLI that comes with the package. They also describe how to use the log files for troubleshooting purposes.

Configuration file

Data Flow service uses `DataflowsConfig.xml` configuration file. The file is located in the default installation path: C:\Program Files (x86)\BigFix Enterprise\Dataflow. The file contains three sections: Data Sources, Data Flows, and Settings. All tags and attribute names in the file must be in lower case. There is also an `DataFlowsConfig.xsd` file that you can use to validate the configuration file on startup.

<datasources>

The `<datasources>` tag of the Configuration File represents a collection of the different data sources that the solution is configured to interact with. For a configuration to be valid, two datasources are required at the minimum. The `<datasourcename>` attribute should be unique.

The `<datasource>` tag is a child node of the `<datasources>` tag in the configuration document and represents the configuration information for a single datasource.

Table 6. Attribute details of the configuration file

Attribute name	Default value	Required	Description
datasourcename	N/A	Yes	This attribute is used to uniquely identify the datasource. With this attribute, datasources can be mapped to specific adapters within each data flow. **Note:** The datasourcename attribute's values should be "TenableSC" or "TenableIO" for Tenable. Ex: <datasource datasource-

Table 6. Attribute details of the configuration file (continued)

Attribute name	Default value	Required	Description
			name="Tenable-IO" .../>
connectionstring	N/A	Yes	URL of the respective data sources. For example: `https://[Qualys-APIURL],https://[TenableAPI_URL]:443` **Note:** Port number is not required for Tenable.io. Ex: https://cloud.tenable.com
username	N/A	System generated	This attribute is managed through the ProvideCredentials command. The data is encrypted prior to being persisted in the configuration file.
password	N/A	System generated	This attribute is managed through the ProvideCredentials command. The data is encrypted prior to being persisted in the configuration file.
verifycert	True	No	This attribute enables or disables SSL certificate validation with this data source.

Table 6. Attribute details of the configuration file (continued)

Attribute name	Default value	Required	Description
			Tenable.sc: If verifycert set to true ensure that the certificates for internal Certificate Authorities (CAs) include the following: • Root Certificates • Intermediate Certificates Default vaule for Tenable.sc is False
proxy_host	N/A	Yes	This attribute provides the proxy server host along with a port number (format: HTTP:// or HTTPS://proxy_host:proxy_port).
proxy_username	N/A	Optional	This attribute is managed through the configureproxy command. The data is encrypted prior to being persisted in the configuration file.
proxy_password	N/A	Optional	This attribute is managed through the configureproxy command. The data is encrypted prior to being persisted in the configuration file.

Note: If the verify cert is set to True in case of proxy, ensure the proxy machine certificate is added to the client of the machine.

<dataflows>

The `<dataflows>` tag of the configuration file represents a collection of the different data flows that the solution is configured to execute.

Each `<dataflow>` tag represents an instance of the flow of data from one system to another and consists of a Source Adapter tag and a Target Adapter tag.

Table 7. Attribute details of the configuration file.

Attribute name	Required	Description
displayname	Yes	This attribute is used to describe the individual data flow.
datatype	Yes	asset (only for Asset Exchange)/finding (for all other dataflows)
schedule*	Yes	Find more information about schedule here

Schedule*

Cron Time String Format: The Cron time string format consists of five fields that Cron converts into a time interval. Cron then uses this interval to determine how often to schedule the DataFlow. 5 place values specify Minute, Hour, Day of the Month, Month, Day of the week respectively.

Character	Descriptor	Acceptable values
1	Minute	**0** to **59**, or *** (no specific value)
2	Hour	**0** to **23**, or *** for any value. The time is your local server time.
3	Day of month	**1** to **31**, or *** (no specific value)
4	Month	**1** to **12**, or *** (no specific value)
5	Day of the week	**0** to **7** (0 and 7 both represent Sunday), or *** (no specific value)

Example usecases:

- Execute data flow after specific minutes past the hour, every hour.
- Execute data flow at specific time of local server time every Monday.
- Execute data flow every five minutes.
- Execute data flow every second hour, on the hour.

Example1: Cron time string of `0 10 15 * *` executes a command on the 15th of each month at 10:00 A.M. local server time.

Example2: Cron time string of `10/30 10 * * *` executes a command on the 10th minute of 10th hour of each day and for every 30 minutes thereafter.

Note: The scheduler value should be configured one minute later to the current time if the dataflow needs to be executed immediately once the start of DataFlows service. For example, if the current time is 11:35:30 the scheduler can be configured to 36 11 * * *.

Note: When initially testing the integration, “now” can be used in the scheduler and Dataflow execution can be tested manually. Once the configuration works, then configure the schedule as per convenience. Ex: schedule = “now”.

<sourceadapter>

The `<sourceadapter>` tag identifies the source system from which the data is extracted. It must include a Properties collection, with a minimum of one property being valid.

Table 8. Attribute details of the configuration file

Attribute name	Required	Description
displayname	Yes	This attribute is used to describe this adapter configuration.
adapterclass	Yes	qualys , tenable, insight (for Asset Exchange only) This attribute determines which adapter is used to extract data from the data source
datasourcename	Yes	This attribute value must match the name of a data source defined in the data sources collection. It is used to provide connection information to the adapter.

<targetadapter>

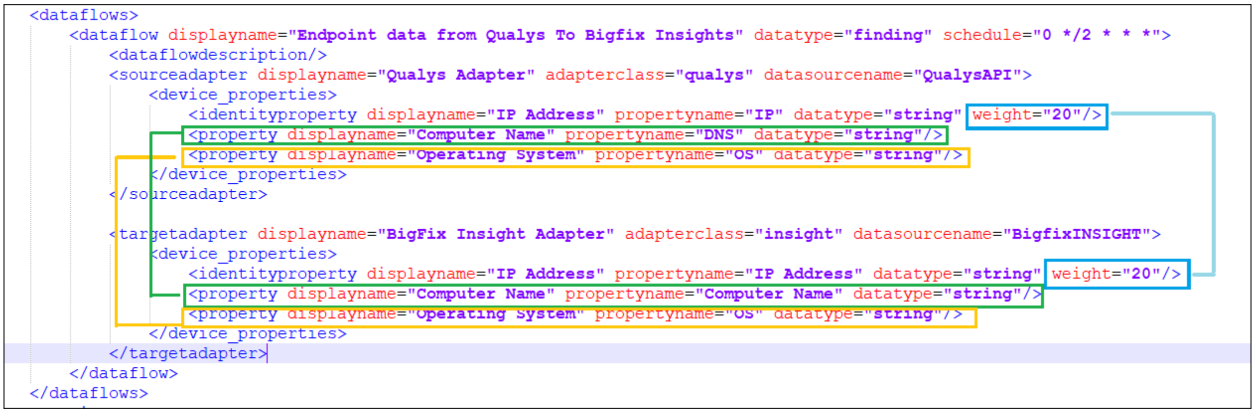
The `<targetadapter>` tag identifies the target system into which the data is loaded. It must include a Properties collection, with a minimum of one property being valid.

Table 9. Attribute details of the configuration file

Attribute name	Required	Description
displayname	Yes	This attribute is used to describe this adapter configuration.
adapterclass	Yes	insight, tenable This attribute determines which adapter is used to extract data from the data source
datasourcename	Yes	This attribute value must match the name of a data source defined in the data sources collection. It is used to provide connection information to the adapter.

<device_properties>

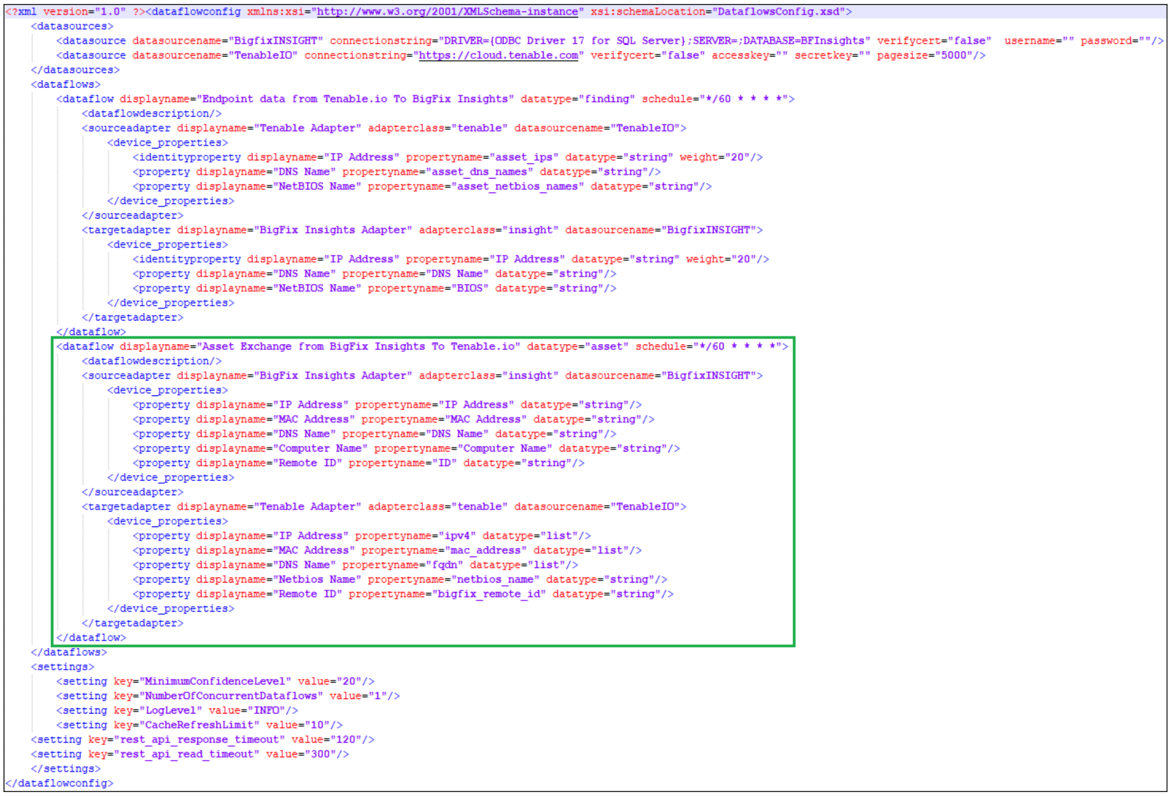
The `<device_properties>` tag represents a collection of properties in a specific adapter. Each property in this collection is mapped by position to the collection in the corresponding target or source adapter. Target and source adapter devices are mapped with weight attribute in <identityproperty> tag.



```
<dataflows>
    <dataflow displayname="Endpoint data from Qualys To Bigfix Insights" datatype="finding" schedule="0 */2 * * *">
        <dataflowdescription/>
        <sourceadapter displayname="Qualys Adapter" adapterclass="qualys" datasourcename="QualysAPI">
            <device_properties>
                <identityproperty displayname="IP Address" propertyname="IP" datatype="string" weight="20"/>
                <property displayname="Computer Name" propertyname="DNS" datatype="string"/>
                <property displayname="Operating System" propertyname="OS" datatype="string"/>
            </device_properties>
        </sourceadapter>

        <targetadapter displayname="BigFix Insight Adapter" adapterclass="insight" datasourcename="BigfixINSIGHT">
            <device_properties>
                <identityproperty displayname="IP Address" propertyname="IP Address" datatype="string" weight="20"/>
                <property displayname="Computer Name" propertyname="Computer Name" datatype="string"/>
                <property displayname="Operating System" propertyname="OS" datatype="string"/>
            </device_properties>
        </targetadapter>
    </dataflow>
</dataflows>
```

Note: By default, there are two dataflows in Tenable.io: Tenable.io dataflow and Asset Exchange dataflow. To disable Asset Exchange dataflow, delete the part of the XML file that includes AE dataflow. **Important**: Dataflow must be deleted from XML file, not commented out.



```
<?xml version="1.0" ?><dataflowconfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="DataflowsConfig.xsd">
    <datasources>
        <datasource datasourcename="BigfixINSIGHT" connectionstring="DRIVER={ODBC Driver 17 for SQL Server};SERVER=;DATABASE=BFInsights" verifycert="false"  username="" password=""/>
        <datasource datasourcename="TenableIO" connectionstring="https://cloud.tenable.com" verifycert="false" accesskey="" secretkey="" pagesize="5000"/>
    </datasources>
    <dataflows>
        <dataflow displayname="Endpoint data from Tenable.io To BigFix Insights" datatype="finding" schedule="*/60 * * * *">
            <dataflowdescription/>
            <sourceadapter displayname="Tenable Adapter" adapterclass="tenable" datasourcename="TenableIO">
                <device_properties>
                    <identityproperty displayname="IP Address" propertyname="asset_ips" datatype="string" weight="20"/>
                    <property displayname="DNS Name" propertyname="asset_dns_names" datatype="string"/>
                    <property displayname="NetBIOS Name" propertyname="asset_netbios_names" datatype="string"/>
                </device_properties>
            </sourceadapter>
            <targetadapter displayname="BigFix Insights Adapter" adapterclass="insight" datasourcename="BigfixINSIGHT">
                <device_properties>
                    <identityproperty displayname="IP Address" propertyname="IP Address" datatype="string" weight="20"/>
                    <property displayname="DNS Name" propertyname="DNS Name" datatype="string"/>
                    <property displayname="NetBIOS Name" propertyname="BIOS" datatype="string"/>
                </device_properties>
            </targetadapter>
        </dataflow>
        <dataflow displayname="Asset Exchange from BigFix Insights To Tenable.io" datatype="asset" schedule="*/60 * * * *">
            <dataflowdescription/>
            <sourceadapter displayname="BigFix Insights Adapter" adapterclass="insight" datasourcename="BigfixINSIGHT">
                <device_properties>
                    <property displayname="IP Address" propertyname="IP Address" datatype="string"/>
                    <property displayname="MAC Address" propertyname="MAC Address" datatype="string"/>
                    <property displayname="DNS Name" propertyname="DNS Name" datatype="string"/>
                    <property displayname="Computer Name" propertyname="Computer Name" datatype="string"/>
                    <property displayname="Remote ID" propertyname="ID" datatype="string"/>
                </device_properties>
            </sourceadapter>
            <targetadapter displayname="Tenable Adapter" adapterclass="tenable" datasourcename="TenableIO">
                <device_properties>
                    <property displayname="IP Address" propertyname="ipv4" datatype="list"/>
                    <property displayname="MAC Address" propertyname="mac_address" datatype="list"/>
                    <property displayname="DNS Name" propertyname="fqdn" datatype="list"/>
                    <property displayname="Netbios Name" propertyname="netbios_name" datatype="string"/>
                    <property displayname="Remote ID" propertyname="bigfix_remote_id" datatype="string"/>
                </device_properties>
            </targetadapter>
        </dataflow>
    </dataflows>
    <settings>
        <setting key="MinimumConfidenceLevel" value="20"/>
        <setting key="NumberOfConcurrentDataflows" value="1"/>
        <setting key="LogLevel" value="INFO"/>
        <setting key="CacheRefreshLimit" value="10"/>
    <setting key="rest_api_response_timeout" value="120"/>
    <setting key="rest_api_read_timeout" value="300"/>
    </settings>
</dataflowconfig>
```

<property>

The `<property>` tag represents a single column of data that is either extracted from or loaded into a system. It may include simple transformation logic to facilitate the transformation of the data received.

Table 10. Attribute details of the configuration file

Attribute name	Required	Description
displayname	Yes	This attribute is used to describe the property being configured.
propertyname	Yes	This attribute is used to identify the corresponding column using a notation specific to each adapter.
datatype	Yes	Type: String
weight	No	This attribute assigns a weight to the property, which is used for the weighted confidence matching of records. Type: Int.

<settings>

The `<settings>` tag represents a collection of settings for the solution. For a detailed list of settings, see Configuration settings for IVR solution.

Table 11. Attribute details of the configuration file

Attribute name	Required	Description
key	Yes	This attribute is the name of the setting that is being configured.
value	yes	This attribute is the value of the setting that is being configured.

Configuration settings for IVR solution

List of available settings you may change in a configuration file.

Setting name	Data type	Default value	Description	Possible values	Remarks
LogLevel	String	DEBUG	Sets the logging level for the service.	• INFO • DEBUG • ERROR	
Ivr_insight.worker_threads	Int	8	Sets the number of worker process (for Correlation) that can be run concurrently.		
Logger.RetentionInDays	Int	5	Indicates the duration of log that you want to retain.		
NumberOfConcurrentDataflows	Int	1	Sets the number of dataflow processors that can be run concurrently.		
DataFlow.QueueRefreshInterval	Int	120	The time interval at which the data flow in refreshed.		

Setting name	Data type	Default value	Description	Possible values	Remarks
MinimumConfidenceLevel	Int	20	The minimum criteria for a record to match.		
CacheRefresh-Limit	Int	10	Configures the system to refresh cache at a specified time interval. Changing this setting may affect the freshness of data with a tradeoff efficient processing of data		
qualys.batch_size	Int	10000	Specifies the maximum number of host records processed per request. When not specified, the `qualys.batch_size` is set to 10,000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000).		
PurgeFindings-OnExecutionOf-Dataflow		FALSE		When set to true, will attempt to purge all *invalid ivr data associated with the current dataflow configuration (from which we	

Setting name	Data type	Default value	Description	Possible values	Remarks
				generate a hash), as well as all data *not* associated with existing dataflow configurations. *invalid - When the user modifies properties of a dataflow, a new hash is calculated. Data in the IVR schema is linked to the configuration hash from which it was derived. **Note:** When the IVR service starts, a purge is performed (regardless of this setting) to attempt to automatically remove all invalid data (again, that is, data	

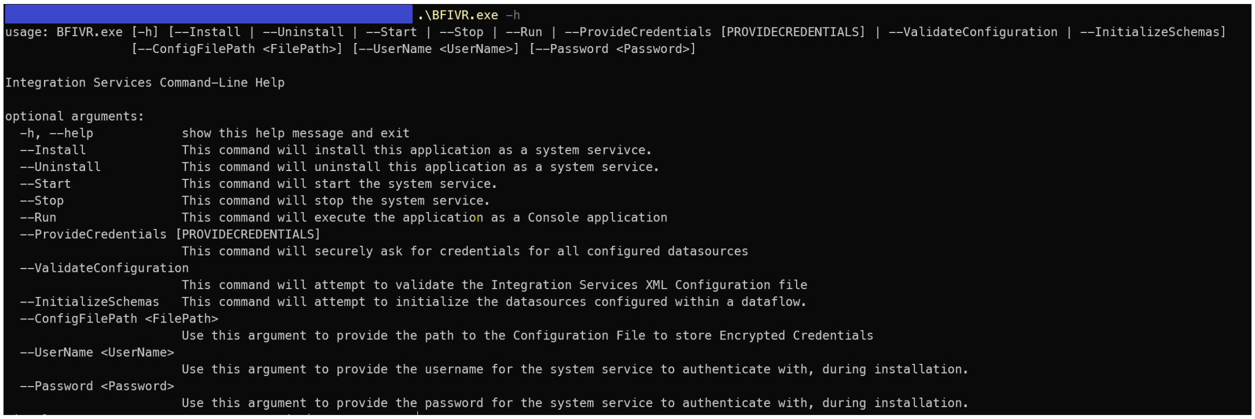
Setting name	Data type	Default value	Description	Possible values	Remarks
				in IVR tables linked to a hash that was calculated from a dataflow configuration that has been changed/modified by the user).	
rest_api_read_timeout	Int	By default none of the timeouts will be set, so it is important to configure values accordingly.	Number of seconds BFIVR waits until connection to a server is established.	Example: <setting key="rest_api_read_timeout" value="5"/>	It is recommended to set connect timeouts slightly larger than a multiple of 3, which is the default TCP packet retransmission window.
rest_api_response	Int		Once BFIVR is connected to a server and HTTP request is sent, this timeout is the number of seconds the user waits for server to respond with data.	Example: <setting key="rest_api_response_timeout" value="5"/>	

Command line interface

The BigFix Insights for Vulnerability Remediation service executable (*BFIVR.exe*) provides a Command Line Interface (CLI) that we can use to perform several distinct functions related to the setup and execution of the solution. This includes installing, uninstalling, starting, and stopping the solution as a native system service. This allows us to securely provide credentials for data sources and validate configuration before starting the service from the BigFix console.

BigFix Insights for Vulnerability Remediation command arguments

The `BFIVR.exe` executable file is found in the default deployment folder. To view a list of all the commands supported, type --Help or -h at the command prompt.



```
[redacted] .\BFIVR.exe -h
usage: BFIVR.exe [-h] [--Install | --Uninstall | --Start | --Stop | --Run | --ProvideCredentials [PROVIDECREDENTIALS] | --ValidateConfiguration | --InitializeSchemas]
                 [--ConfigFilePath <FilePath>] [--UserName <UserName>] [--Password <Password>]

Integration Services Command-Line Help

optional arguments:
  -h, --help            show this help message and exit
  --Install             This command will install this application as a system servivce.
  --Uninstall           This command will uninstall this application as a system service.
  --Start               This command will start the system service.
  --Stop                This command will stop the system service.
  --Run                 This command will execute the application as a Console application
  --ProvideCredentials [PROVIDECREDENTIALS]
                        This command will securely ask for credentials for all configured datasources
  --ValidateConfiguration
                        This command will attempt to validate the Integration Services XML Configuration file
  --InitializeSchemas   This command will attempt to initialize the datasources configured within a dataflow.
  --ConfigFilePath <FilePath>
                        Use this argument to provide the path to the Configuration File to store Encrypted Credentials
  --UserName <UserName>
                        Use this argument to provide the username for the system service to authenticate with, during installation.
  --Password <Password>
                        Use this argument to provide the password for the system service to authenticate with, during installation.
```

Table 12. List of command line arguments

Command	Purpose	Additional information
--ProvideCredentials <DataSourceName>	To securely capture credentials for single datasource	
--provideCredentials	To securely capture credentials for all datasources	
--ValidateConfiguration	To validate the configuration	
--InitializeSchemas	To initialize the schema	
--configureproxy	To configure proxy parameters	

Note: The command line parameters are case sensitive.

Logs

You can find log files in the `logs` folder in the installation path. Logs are updated every day. Configure the solution with INFO as the log level unless you intend to troubleshoot an issue.

Connections.[date].log

With DEBUG enabled, this log file contains detailed logging information related to the external connections to third-party datasources.

DataFlow.[date].log

With DEBUG enabled, this log file contains detailed logging information related to the execution of each dataflow. It is the primary interface used for debugging issues related to the ETL (Extract, Transform, Load)..

Main.[date]log

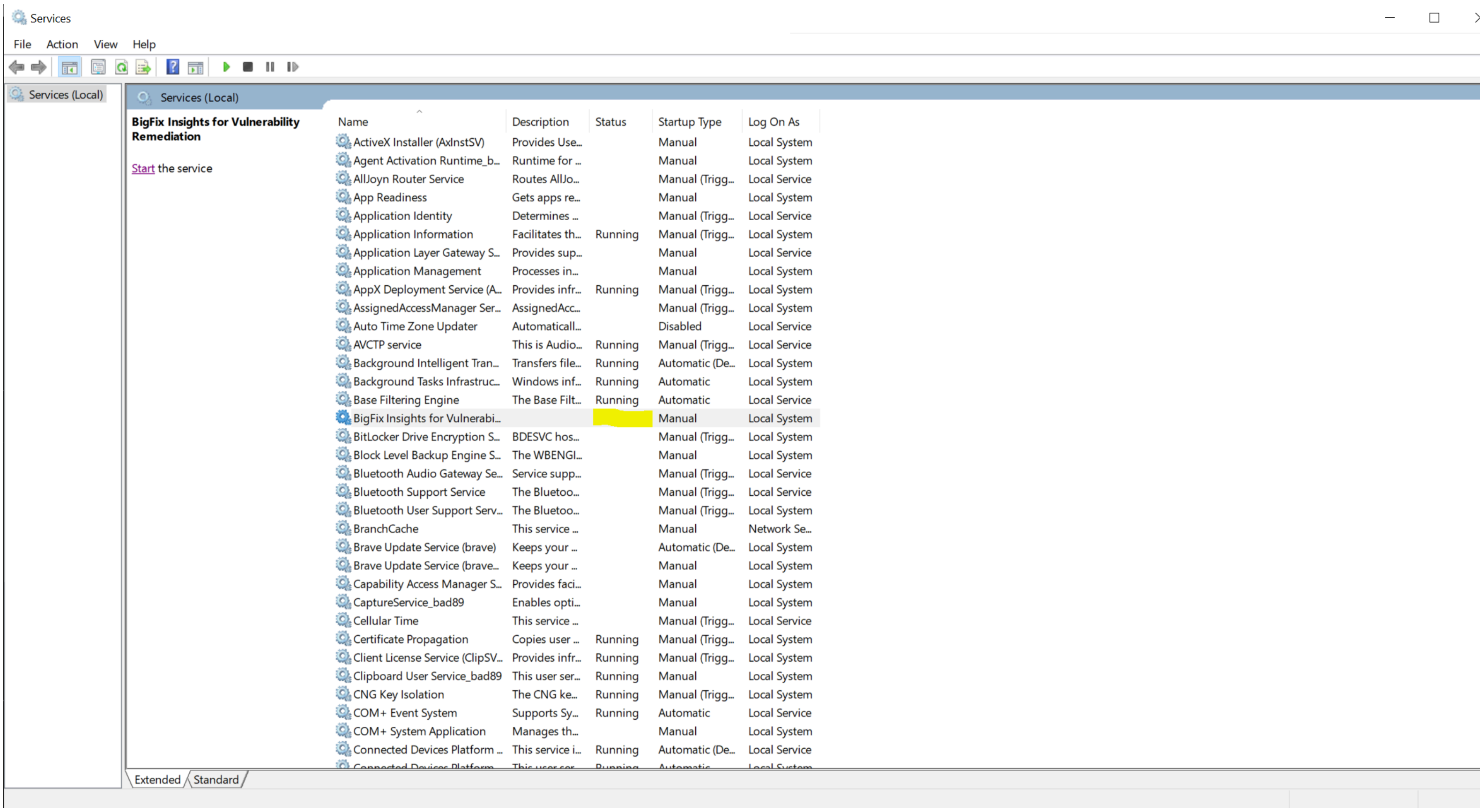
With DEBUG enabled, this log file contains detailed logging information related to the primary processes. It should show issues related to service start and configuration.

Troubleshooting

This topic helps you in troubleshooting various issues encountered in IVR (BigFix Insights for Vulnerability Remediation) service.

Diagnostic procedures:

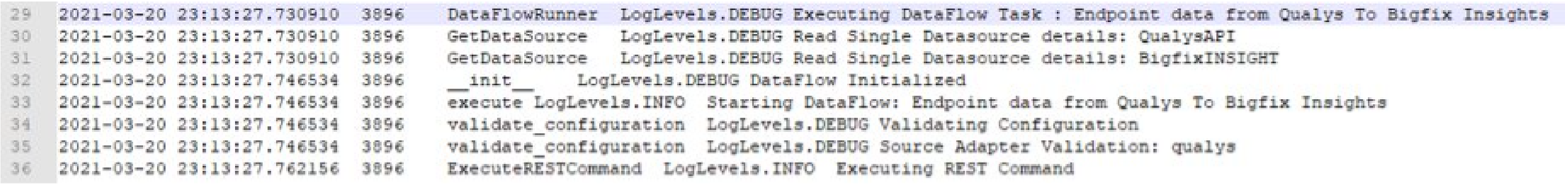
- Check Windows Service Manager for Service State. The service should be in a running state.



Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Use...		Manual	Local System
Agent Activation Runtime_b...	Runtime for ...		Manual	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trigg...	Local Service
App Readiness	Gets apps re...		Manual	Local System
Application Identity	Determines ...		Manual (Trigg...	Local Service
Application Information	Facilitates th...	Running	Manual (Trigg...	Local System
Application Layer Gateway S...	Provides sup...		Manual	Local Service
Application Management	Processes in...		Manual	Local System
AppX Deployment Service (A...	Provides infr...	Running	Manual (Trigg...	Local System
AssignedAccessManager Ser...	AssignedAcc...		Manual (Trigg...	Local System
Auto Time Zone Updater	Automaticall...		Disabled	Local Service
AVCTP service	This is Audio...	Running	Manual (Trigg...	Local Service
Background Intelligent Tran...	Transfers file...	Running	Automatic (De...	Local System
Background Tasks Infrastruc...	Windows inf...	Running	Automatic	Local System
Base Filtering Engine	The Base Filt...	Running	Automatic	Local Service
BigFix Insights for Vulnerabi...			Manual	Local System
BitLocker Drive Encryption S...	BDESVC hos...		Manual (Trigg...	Local System
Block Level Backup Engine S...	The WBENGI...		Manual	Local System
Bluetooth Audio Gateway Se...	Service supp...		Manual (Trigg...	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trigg...	Local Service
Bluetooth User Support Serv...	The Bluetoo...		Manual (Trigg...	Local System
BranchCache	This service ...		Manual	Network Se...
Brave Update Service (brave)	Keeps your ...		Automatic (De...	Local System
Brave Update Service (brave...	Keeps your ...		Manual	Local System
Capability Access Manager S...	Provides faci...		Manual	Local System
CaptureService_bad89	Enables opti...		Manual	Local System
Cellular Time	This service ...		Manual (Trigg...	Local Service
Certificate Propagation	Copies user ...	Running	Manual (Trigg...	Local System
Client License Service (ClipSV...	Provides infr...	Running	Manual (Trigg...	Local System
Clipboard User Service_bad89	This user ser...	Running	Manual	Local System
CNG Key Isolation	The CNG ke...	Running	Manual (Trigg...	Local System
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...		Manual	Local System
Connected Devices Platform ...	This service i...	Running	Automatic (De...	Local Service
Connected Devices Platform ...	This user ser...	Running	Automatic	Local System

- Check logs for errors & timestamp. Logs are found in the logs directory.

[DatetimeOfExecution] [ProcessID] [Method] [Message]



```
2021-03-20 23:13:27.730910  3896    DataFlowRunner  LogLevels.DEBUG Executing DataFlow Task : Endpoint data from Qualys To Bigfix Insights
2021-03-20 23:13:27.730910  3896    GetDataSource   LogLevels.DEBUG Read Single Datasource details: QualysAPI
2021-03-20 23:13:27.730910  3896    GetDataSource   LogLevels.DEBUG Read Single Datasource details: BigfixINSIGHT
2021-03-20 23:13:27.746534  3896    __init__    LogLevels.DEBUG DataFlow Initialized
2021-03-20 23:13:27.746534  3896    execute LogLevels.INFO  Starting DataFlow: Endpoint data from Qualys To Bigfix Insights
2021-03-20 23:13:27.746534  3896    validate_configuration  LogLevels.DEBUG Validating Configuration
2021-03-20 23:13:27.746534  3896    validate_configuration  LogLevels.DEBUG Source Adapter Validation: qualys
2021-03-20 23:13:27.762156  3896    ExecuteRESTCommand  LogLevels.INFO  Executing REST Command
```

Table 13. DataFlow logs details

Message	Description
Executing DataFlow Task: Endpoint data from Qualys to BigFix Insights	Indicates start of data flow
Loading Qualys Data	Indicates loading of Qualys data
Loading Insights Data	Indicates loading of Insights data
RecordCaches Loaded In	Indicates time it took to get data from Insights and Source Adapter (Qualys or Tenable)
Processing Changes From Source Adapter	At this point, we will take the changes and prepare updates for the IVR tables. The time when the processing changes from source adapter are considered and are updated in the IVR tables.
Done Processing Devices	Indicates that the device correlation is complete.
Updates Performed In	Indicates the time taken to stick data in the IVR tables.
Saving RecordCaches	The final step in which the record cache is saved.
DataFlowExecution Completed In	Indicates the end of data flow.
Starting Dataflow: Endpoint data from Tenable.io to Bigfix Insights	Indicates start of data flow
Connected to Tenable.io Server VERSION 6.9.1	Indicates loading of Tenable data is about to start

- Setting Verbosity - refer to the link for more information.

Known limitations

Refer to the below list of limitations in BigFix Insights for Vulnerability Remediation.

⚠ **Warning:** Do not use more than 1 dataflow per BigFix Insights for Vulnerability Remediation service.

⚠ **Warning:** Do not deploy BigFix Insights for Vulnerability Remediation service to more than 1 machine.

1. IVR(BigFix Insights for Vulnerability Remediation)1.1 currently officially supports BigFix Insights instances with only one BigFix Datasource.
2. IVR Tenable.sc: Allow Session Management must be disabled. For more information, refer to the Tenable.sc configuration settings.
3. Currently we do not support multi-instance data flow service even for the same datasource type.
4. PowerBI and Tableau reports: The maximum number of records which can be exported to CSV file:
    - 50k records for Tableau
    - 30k records for PowerBI
5. Power BI: The sorting of severities in the breakdown vizualizations may yield unpredictable results.
    - Sort order of the bars come up differently in an unpredictable order, but does not affect the functionality of the data.
6. IVR Tenable.io: Findings in the IVR.findings table whose asset has been deleted on Tenable.io are not removed until the finding/vulnerabilities themselves are updated on Tenable.io.
7. To run Asset Exchange and Tenable.io, the service should be stopped and restarted in between an Asset Exchange dataflow and Tenable.io dataflow.
8. Tenable.io: IP Addresses Multiplicity - If a property result set for a given device/asset contains more than one IPv4 address, this device/asset is not correlated. Currently not supported.
9. IVR Insights: Deleted custom fixlets remain in the IVR.vulnerability_fixlet_nexus table.
10. The drill-through filter to the Vulnerability List from the Overview dashboard for the Date Detected/Published visualization may not work correctly.

Chapter 11. Release Notes

The **release notes** outline the features, updates and patches that are included in each version of BigFix Insights for Vulnerability Remediation, including the latest application updates.

IVR 2.0.3 Release Notes

The BigFix team is pleased to announce the release of version 2.0.3 of the BigFix Insights for Vulnerability Remediation application (included in the BigFix Lifecycle and Compliance sites). This application will enable IT Security and Operations teams to collaborate much more effectively by automatically correlating discovered vulnerabilities to their proper remediations, while providing prioritization data to focus remediation efforts.

The main features of this release are as follows:

- Security improvements
- Bugfixes
- User agent support for Tenable.sc

Additional information about this release:

- Please find the **BigFix Insights for Vulnerability Remediation** Fixlet Site from the License Overview Dashboard under the Lifecycle or Compliance Sections.

  For more information on enabling sites, please see https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Console/c_license_overview_dashboard.html
- Published site version: 13

Useful links

- Documentation: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html
- Insights for Vulnerability Remediation Schema: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Schema/c_IVR_schema.html
- Learn more on our Product Page: https://www.hcltechsw.com/bigfix/ivr-home

IVR 1.4 Release Notes

The BigFix team is pleased to announce the release of version 1.4 of the BigFix Insights for Vulnerability Remediation application (included in the BigFix Lifecycle and Compliance sites). This application will enable IT Security and Operations teams to collaborate much more effectively by automatically correlating discovered vulnerabilities to their proper remediations, while providing prioritization data to focus remediation efforts.

The main features of this release are as follows:

- Simplified Deployment, Configuration, and Management of IVR through Fixlets
    - You can now deploy as well as configure IVR through a single Fixlet to get up and running that much more quickly and easily! For more information, please see the Deployment and configuration section of the documentation
    - Additional Tasks are available to simplify general management of IVR including data synchronization schedules, credentials, and service states. Please see the IVR Fixlets and Tasks section of the documentation for more information

Additional information about this release:

- Please find the **BigFix Insights for Vulnerability Remediation** Fixlet Site from the License Overview Dashboard under the Lifecycle or Compliance Sections

  For more information on enabling sites, please see https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Console/c_license_overview_dashboard.html

- Published site version: 10

Useful links

- Documentation: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html

- Insights for Vulnerability Remediation Schema: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Schema/c_IVR_schema.html

- Learn more on our Product Page: https://www.hcltechsw.com/bigfix/ivr-home

IVR 1.3 Release Notes

The BigFix team is pleased to announce the release of version 1.3 of the BigFix Insights for Vulnerability Remediation application (included in the BigFix Lifecycle and Compliance suites). This application will enable IT Security and Operations teams to collaborate much more effectively by automatically correlating discovered vulnerabilities to their proper remediations, while providing prioritization data to focus remediation efforts.

The main features of this release are as follows:

- Introduced support for Tenable.sc version 5.20.x

Additional information about this release:

- Please find the **BigFix Insights for Vulnerability Remediation** Fixlet Site from the License Overview Dashboard under the Lifecycle or Compliance Sections

  For more information on enabling sites, please see https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Console/c_license_overview_dashboard.html

- Published site version: 9

Useful links

- Documentation: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html
- Insights for Vulnerability Remediation Schema: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Schema/c_IVR_schema.html
- Learn more on our Product Page: https://www.hcltechsw.com/bigfix/ivr-home

IVR 1.2 Release Notes

The BigFix team is pleased to announce the release of version 1.2 of the BigFix Insights for Vulnerability Remediation application (included in the BigFix Lifecycle and Compliance suites). This application will enable IT Security and Operations teams to collaborate much more effectively by automatically correlating discovered vulnerabilities to their proper remediations, while providing prioritization data to focus remediation efforts.

The main features of this release are as follows:

- Better scheduling support
  - You can now define granular schedules for BigFix Insights for Vulnerability Remediation to better control and manage when data will be synchronized and processed
- Proxy support
  - Connections from BigFix Insights for Vulnerability Remediation to your vulnerability management products can now be directed through a proxy for improved security
- Other minor enhancements and bug fixes

Additional information about this release:

- Find the **BigFix Insights for Vulnerability Remediation** Fixlet Site from the License Overview Dashboard under the Lifecycle or Compliance Sections

  For more information on enabling sites, please see https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Console/c_license_overview_dashboard.html

Useful links

- Documentation: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Install_Config/c_welcome.html
- Insights for Vulnerability Remediation Schema: https://help.hcltechsw.com/bigfix/10.0/integrations/Ecosystem/Schema/c_IVR_schema.html
- Learn more on our Product Page: https://www.hcltechsw.com/bigfix/ivr-home

Appendix A. Glossary

This glossary provides terms and definitions for the Modern Client Management for BigFix software and products.

The following cross-references are used in this glossary:

- *See* refers you from a non-preferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

A B C D E F G L M N O P R S T U V W

A

action

1. See Fixlet.
2. A set of Action Script commands that perform an operation or administrative task, such as installing a patch or rebooting a device.

Action Script

Language used to perform an action on an endpoint.

agent

See BigFix agent.

ambiguous software

Software that has an executable file that looks like another executable file, or that exists in more than one place in a catalog (Microsoft Word as a standalone product or bundled with Microsoft Office).

audit patch

A patch used to detect conditions that cannot be remediated and require the attention of an administrator. Audit patches contain no actions and cannot be deployed.

automatic computer group

A computer group for which membership is determined at run time by comparing the properties of a given device against the criteria set for group membership. The set of devices in an automatic group is dynamic, meaning that the group can and does change. See also computer group.

B

baseline

A collection of actions that are deployed together. A baseline is typically used to simplify a deployment or to control the order in which a set of actions are applied. See also deployment group.

BigFix agent

The BigFix code on an endpoint that enables management and monitoring by BigFix.

BigFix client

See BigFix agent.

BigFix console

The primary BigFix administrative interface. The console provides a full set of capabilities to BigFix administrators.

BYOD

Bring Your Own Device (BYOD) refers to employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data.

C

client

A software program or computer that requests services from a server. See also server.

client time

The local time on a BigFix client device.

Cloud

A set of compute and storage instances or services that are running in containers or on virtual machines.

Common Vulnerabilities and Exposures Identification Number (CVE ID)

A number that identifies a specific entry in the National Vulnerability Database. A vendor's patch document often includes the CVE ID, when it is available. See also National Vulnerability Database.

Common Vulnerabilities and Exposures system (CVE)

A reference of officially known network vulnerabilities, which is part of the National Vulnerabilities Database (NVD), maintained by the US National Institute of Standards and Technology (NIST).

component

An individual action within a deployment that has more than one action. See also deployment group.

computer group

A group of related computers. An administrator can create computer groups to organize systems into meaningful categories, and to facilitate deployment of content to multiple computers. See also automatic computer group and manual computer group.

console

See BigFix console.

content

Digitally-signed files that contain data, rules, queries, criteria, and other instructions, packaged for deployment across a network. BigFix agents use the detection criteria (Relevance statements) and action instructions (Action Script statements) in content to detect vulnerabilities and enforce network policies.

content relevance

A determination of whether a patch or piece of software is eligible for deployment to one or more devices. See also device relevance.

Coordinated Universal Time (UTC)

The international standard of time that is kept by atomic clocks around the world.

corrupt patch

A patch that flags an operator when corrections made by an earlier patch have been changed or compromised. This situation can occur when an earlier service pack or application overwrites later files, which results in patched files that are not current. The corrupt patch flags the situation and can be used to re-apply the later patch.

custom content

BigFix code that is created by a customer for use on their own network, for example, a custom patch or baseline.

CVE

See Common Vulnerabilities and Exposures system.

CVE ID

See Common Vulnerabilities and Exposures Identification Number.

D

data stream

A string of information that serves as a source of package data.

default action

The action designated to run when a Fixlet is deployed. When no default action is defined, the operator is prompted to choose between several actions or to make an informed decision about a single action.

definitive package

A string of data that serves as the primary method for identifying the presence of software on a computer.

deploy

To dispatch content to one or more endpoints for execution to accomplish an operation or task, for example, to install software or update a patch.

deployment

Information about content that is dispatched to one or more endpoints, a specific instance of dispatched content.

deployment group

The collection of actions created when an operator selects more than one action for a deployment, or a baseline is deployed. See also baseline, component, deployment window, and multiple action group.

deployment state

The eligibility of a deployment to run on endpoints. The state includes parameters that the operator sets, such as 'Start at 1AM, end at 3AM.'

deployment status

Cumulative results of all targeted devices, expressed as a percentage of deployment success.

deployment type

An indication of whether a deployment involved one action or multiple actions.

deployment window

The period during which a deployment's actions are eligible to run. For example, if a Fixlet has a deployment window of 3 days and an eligible device that has been offline reports in to BigFix within the 3-day window, it gets the Fixlet. If the device comes back online after the 3-day window expires, it does not get the Fixlet. See also deployment group.

device

An endpoint, for example, a laptop, desktop, server, or virtual machine that BigFix manages; an endpoint running the BigFix Agent.

device holder

The person using a BigFix-managed computer.

device property

Information about a device collected by BigFix, including details about its hardware, operating system, network status, settings, and BigFix client. Custom properties can also be assigned to a device.

device relevance

A determination of whether a piece of BigFix content applies to applies to a device, for example, where a patch should be applied, software installed, or a baseline run. See also content relevance.

device result

The state of a deployment, including the result, on a particular endpoint.

Disaster Server Architecture (DSA)

An architecture that links multiple servers to provide full redundancy in case of failure.

DSA

See Disaster Server Architecture.

dynamically targeted

Pertaining to using a computer group to target a deployment.

E

endpoint

A networked device running the BigFix agent.

F

filter

To reduce a list of items to those that share specific attributes.

Fixlet

A piece of BigFix content that contains Relevance and Action Script statements bundled together to perform an operation or task. Fixlets are the basic building blocks of BigFix content. A Fixlet provides instructions to the BigFix agent to perform a network management or reporting action.

Full Disk Encryption

To reduce a list of items to those that share specific attributes.

G

group deployment

A type of deployment in which multiple actions were deployed to one or more devices.

L

locked

An endpoint state that prevents most of the BigFix actions from running until the device is unlocked.

M

MAG

See multiple action group.

management rights

The limitation of console operators to a specified group of computers. Only a site administrator or a master operator can assign management rights.

manual computer group

A computer group for which membership is determined through selection by an operator. The set of devices in a manual group is static, meaning they do not change. See also computer group.

master operator

A console operator with administrative rights. A master operator can do everything that a site administrator can do, except creating operators.

masthead

A collection of files that contain the parameters of the BigFix process, including URLs to Fixlet content. The BigFix agent brings content into the enterprise based on subscribed mastheads.

MCM and BigFix Mobile

Refers to the offering by Bigfix that is common for both Modern Client Management to manage laptops (Windows and macOS) and BigFix Mobile to manage mobile devices (Android, iOS, and iPadOS).

mirror server

A BigFix server required if the enterprise does not allow direct web access but instead uses a proxy server that requires password-level authentication.

Multicloud

The utilization of distinct sets of cloud services, typically from multiple vendors, where specific applications are confined to a single cloud instance.

multiple action group (MAG)

A BigFix object that is created when multiple actions are deployed together, as in a baseline. A MAG contains multiple Fixlets or tasks. See also deployment group.

N

National Vulnerability Database (NVD)

A catalog of officially known information security vulnerabilities and exposures, which is maintained by the National Institute of Standards and Technology (NIST). See also Common Vulnerabilities and Exposures Identification Number.

NVD

See National Vulnerability Database.

O

offer

A deployment option that allows a device holder to accept or decline a BigFix action and to exercise some control over when it runs. For example, a device holder can decide whether to install a software application, and whether to run the installation at night or during the day.

open-ended deployment

A deployment with no end or expiration date; one that runs continuously, checking whether the computers on a network comply.

operator

A person who uses the BigFix WebUI, or portions of the BigFix console.

P

patch

A piece of code added to vendor software to fix a problem, as an immediate solution that is provided to users between two releases.

patch category

A description of a patch's type and general area of operation, for example, a bug fix or a service pack.

patch severity

The level of risk imposed by a network threat or vulnerability and, by extension, the importance of applying its patch.

R

relay

A client that is running special server software. Relays spare the server and the network by minimizing direct server-client downloads and by compressing upstream data.

Relevance

BigFix query language that is used to determine the applicability of a piece of content to a specified endpoint. Relevance asks yes or no questions and evaluates the results. The result of a Relevance query determines whether an action can or should be applied. Relevance is paired with Action Script in Fixlets.

S

SCAP

See Security Content Automation Protocol.

SCAP check

A specific configuration check within a Security Content Automation Protocol (SCAP) checklist. Checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

SCAP checklist

A configuration checklist that is written in a machine-readable language (XCCDF). Security Content Automation Protocol (SCAP) checklists have been submitted to and accepted by the NIST National Checklist Program. They also conform to a SCAP template to ensure compatibility with SCAP products and services.

SCAP content

A repository that consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

SCAP enumeration

A list of all known security related software flaws (CVEs), known software configuration issues (CCEs), and standard vendor and product names (CPEs).

SCAP mapping

The interrelationship of enumerations that provides standards-based impact measurements for software flaws and configuration issues.

Security Content Automation Protocol (SCAP)

A set of standards that is used to automate, measure, and manage vulnerability and compliance by the National Institute of Standards and Technology (NIST).

server

A software program or a computer that provides services to other software programs or other computers. See also client.

signing password

A password that is used by a console operator to sign an action for deployment.

single deployment

A type of deployment where a single action was deployed to one or more devices.

site

A collection of BigFix content. A site organizes similar content together.

site administrator

The person who is in charge of installing BigFix and authorizing and creating new console operators.

software package

A collection of Fixlets that install a software product on a device. Software packages are uploaded to BigFix by an operator for distribution. A BigFix software package includes the installation files, Fixlets to install the files, and information about the package (metadata).

SQL Server

A full-scale database engine from Microsoft that can be acquired and installed into the BigFix system to satisfy more than the basic reporting and data storage needs.

standard deployment

A deployment of BigFix that applies to workgroups and to enterprises with a single administrative domain. It is intended for a setting in which all Client computers have direct access to a single internal server.

statistically targeted

Pertaining to the method used to target a deployment to a device or piece of content. Statically targeted devices are selected manually by an operator.

superseded patch

A type of patch that notifies an operator when an earlier version of a patch has been replaced by a later version. This occurs when a later patch updates the same files as an earlier one. Superseded patches flag vulnerabilities that can be remediated by a later patch. A superseded patch cannot be deployed.

system power state

A definition of the overall power consumption of a system. BigFix Power Management tracks four main power states Active, Idle, Standby or Hibernation, and Power Off.

T

target

To match content with devices in a deployment, either by selecting the content for deployment, or selecting the devices to receive content.

targeting

The method used to specify the endpoints in a deployment.

task

A type of Fixlet designed for re-use, for example, to perform an ongoing maintenance task.

U

UTC

See Coordinated Universal Time.

V

virtual private network (VPN)

An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

VPN

See virtual private network.

vulnerability

A security exposure in an operating system, system software, or application software component.

W

Wake-from-Standby

A mode that allows an application to turn a computer on from standby mode during predefined times, without the need for Wake on LAN.

Wake on LAN

A technology that enables a user to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, users of this technology can remotely turn on a server and control it across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

WAN

See wide area network.

wide area network (WAN)

A network that provides communication services among devices in a geographic area larger than that served by a local area network (LAN) or a metropolitan area network (MAN).

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.