

# **BigFix Compliance QRadar User's Guide**



# Special notice

Before using this information and the product it supports, read the information in [Notices \(on page 21\)](#).

# **Edition notice**

This edition applies to version 9.5 of BigFix and to all subsequent releases and modifications until otherwise indicated in new editions.

# Contents

<b>Chapter 1. Overview and getting started.....</b>	<b>1</b>
At a glance.....	1
Operator permissions.....	3
Requirements.....	3
Accessing the site.....	5
Install the plug-in.....	5
Uninstalling.....	7
<b>Chapter 2. Remediate vulnerabilities.....</b>	<b>9</b>
Computer details.....	9
Quarantining computers.....	11
Un-quarantining computers.....	13
Viewing Common Vulnerability Exposures (CVEs) and associated Fixlets.....	14
Viewing actions.....	17
Troubleshooting.....	17
<b>Chapter 3. Support.....</b>	<b>20</b>
Notices.....	21

# Chapter 1. Overview and getting started

HCL® BigFix provides the **Manage Vulnerable Computers** dashboard from which you can view and remediate QRadar® vulnerability data. The dashboard lists the QRadar® Computer Risk Score, CVEs, and CVE risk score, which you can use to quickly identify the computers that are at risk. The dashboard provides a list of the Fixlets and Baselines that are available to take action and remediate CVEs. You can also quarantine or unquarantine computers from the Manage Vulnerable Computers **Manage Vulnerable Computers** dashboard. An **Actions** tab shows the actions that you ran from the dashboard.

If you have QRadar® Vulnerability Manager installed and configured to connect to BigFix and if you have a license for BigFix Compliance, you can access the **Manage Vulnerable Computers** dashboard. You begin by installing a plug-in in BigFix. After you install the plug-in, you can use the dashboard.

To use the **Manage Vulnerable Computers** dashboard, you must complete two simple steps in BigFix:

1. Acquire the QRadar Vulnerabilities site. See [Accessing the site \(on page 5\)](#).
2. Install the plug-in for the **Manage Vulnerable Computers** dashboard. See [Install the QRadar® plug-in \(on page 5\)](#).

Use the documentation in the following sections to complete each of these tasks in BigFix.

 **Important:** Before completing these tasks in BigFix, you must also complete some short configuration steps in QRadar® to enable QRadar® to send vulnerability data to BigFix. For information about the configuration that is required in QRadar®, see the [QRadar and BigFix integration](#) wiki.

## At a glance: Manage Vulnerable Computers dashboard

The **Manage Vulnerable Computers** dashboard identifies the QRadar® Computer Risk Score for each of the computers that you manage in BigFix. The dashboard also identifies the

CVSS risk score associated with each CVE. Using this enriched risk assessment data from QRadar®, you can immediately identify the computers that are most at risk. The dashboard provides a list of the Fixlets and Baselines that are available for CVEs. You can run Fixlets or Baselines from the **Manage Vulnerable Computers** dashboard to remediate vulnerabilities and secure the vulnerable computers.

QRadar® connects to BigFix and sends vulnerability data to the BigFix server. The **Manage Vulnerable Computers** dashboard displays this enriched risk assessment data. The following graphic shows the **Computers** view of the **Manage Vulnerable Computers** dashboard. The **Show Computers that have Relevant Fixlets** check box is selected, which filters the list of computers to those for which there are remediation Fixlets or Baselines available. In the computers list, the **QRadar Computer Risk Score** provides enriched risk assessment information for you to immediately identify the computers that are most at risk. In the CVEs list part of the screen, the **CVSS Risk Score** identifies the CVE with the highest risk score for the computer that is selected in the computers list.

Computer ID	Computer Name	Operating System	Quarantine Status	QRadar Computer Risk Score	Actionable CVEs	CVEs
10586687	SIMULATEDCOMPUTER_18095	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23
10231556	SIMULATEDCOMPUTER_59940	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23
12001451	SIMULATEDCOMPUTER_120021	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23
12047866	SIMULATEDCOMPUTER_120022	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23
10147861	SIMULATEDCOMPUTER_120115	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23
12134515	SIMULATEDCOMPUTER_120193	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23
11246042	SIMULATEDCOMPUTER_120196	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23
12205519	SIMULATEDCOMPUTER_120211	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23
11611578	SIMULATEDCOMPUTER_59923	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23
10383637	SIMULATEDCOMPUTER_120233	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23
10873581	SIMULATEDCOMPUTER_120316	Linux Red Hat Enterprise Server 7.2 (3.10...)	Not Applicable	23.00	23	23

  

CVE ID	CVSS Risk Score
2016-5696	1.00
2016-5403	1.00
2016-5126	1.00
2016-5699	1.00
2016-1000110	1.00
2016-0772	1.00
2016-5444	1.00
2016-5440	1.00
2016-3615	1.00
2016-3521	1.00
2016-3477	1.00
2016-3452	1.00

In the lower part of the screen, the CVEs associated with the selected computer are displayed. The **Relevant Fixlets** tab shows the Fixlets and Baselines that are available to remediate the selected CVE.

To run a Fixlet or Baseline to remediate the CVE, you click **Take Default Action**.

## Operator permissions for the **Manage Vulnerable Computers** dashboard

Operators accessing the BigFix **Manage Vulnerable Computers** dashboard and Fixlet APIs must have particular read/write permissions. Master operators can use the BigFix Console to change or assign permissions for operators as required.

For more information about BigFix permissions, see: [Operators permissions](#).

Complete the following steps to set the required BigFix permissions.

1. In the BigFix Console, navigate to **All Content > Operators**.
2. Select the Operator for which you want to assign permissions.
3. Navigate to the **Details** tab and set the following permissions if necessary:
  - a. Under **Permissions**, change **Custom Content** to **Yes**.
  - b. Under **Interface Login Privileges**, change **Can use REST API** to **Yes**.
4. Save the changes.

## Requirements

Ensure that your system meets the requirements for the **Manage Vulnerable Computers** dashboard to operate correctly.

The **Manage Vulnerable Computers** dashboard has the following requirements:

- BigFix console version 9.2.6 is recommended.
- BigFix client version 9.2.6 or later is required.

- The **BES Server Plugin Service** must be installed on the BigFix server and must be configured correctly.
- BigFix Web Reports must be set up and running for the QRadar® plug-in to operate correctly. For information about configuring Web Reports, see [Web Reports Guide](#).
- Your computers must be subscribed to the site that contains the Fixlet and patch content.
- If you are not a master operator, you must be subscribed to the site that contains the Fixlet and patch content to remediate CVEs.
- As an operator, you must be subscribed to the **Patching Support** site.
- You must activate the **Quarantine Status** analysis from **Manage Vulnerabilities > Setup and Maintenance > Activate Analyses**.
- As an operator, you must have permissions to manage the computers that are subscribed to the site. For information about how operators are assigned permissions to computers, see [Operator's permissions](#).
- To quarantine and un-quarantine computers, you must set up a policy action for both the Quarantine and Un-quarantine Fixlets. To set up the policy actions, use the following example, which shows how to set up the policy action for the quarantine Fixlet to quarantine computers:
  1. From the **Endpoint Protection** domain, select **Manage Vulnerabilities > Setup and Maintenance > Fixlets and Tasks**.
  2. Select the **Quarantine Microsoft Windows** computers Fixlet and review the information in the Fixlet description.
  3. Click **Take Action**.
  4. On the **Targets** tab in the **Take Action** dialog, select the **Dynamically target by property** option, and select **All Computers**.
  5. On the **Execution** tab, clear the **Ends on** check box, check the **Reapply this action** check box with the **whenever it becomes relevant again** option selected, and clear the **Limit to** check box.
  6. Click **OK** to set up the policy action.Complete a similar procedure to set up the policy action for the un-quarantine Fixlet. Set up the un-quarantine policy action on the **Un-quarantine Microsoft Windows**

**computers** Fixlet from **Manage Vulnerabilities > Setup and Maintenance > Fixlets and Tasks**.

## Accessing the site

The **Manage Vulnerable Computers** dashboard runs from the BigFix **Endpoint Protection** domain. Before you can access the **Manage Vulnerable Computers** dashboard, you must acquire the QRadar Vulnerabilities site and accept the license agreement. After you acquire the QRadar Vulnerabilities site, you must gather the contents of the site to your console. You must also subscribe your computers to the site so that they can access the **Manage Vulnerable Computers** dashboard.

You cannot access the QRadar Vulnerabilities site unless you have a license for BigFix Compliance. For information about getting a license, see [BigFix Licensing](#).

The procedure for acquiring the QRadar Vulnerabilities site and gathering the contents of the site is similar to the procedure for other BigFix applications and sites.

Complete the following steps to access the site.

1. From the BigFix console, go to the **BigFix Management** domain and click **License Overview**.
2. Go to the BigFix Compliance section of the **License Overview** dashboard.
3. Click **Enable** for the QRadar Vulnerabilities site. The QRadar® site is made available on your console. It typically takes a few minutes for the contents to become available on your system.
4. From the **All Content** domain, subscribe the computers that you want to manage from the **Manage Vulnerable Computers** dashboard to the QRadar Vulnerabilities site.

## Install the QRadar® plug-in

Before you can access the QRadar® vulnerability data from the BigFix console, you must install the QRadar® plug-in in BigFix. To install the QRadar® plug-in, you run a Fixlet.

There is a separate installation Fixlet available for Windows and Linux. When running the installation Fixlet, you must target the BigFix server. After you have installed the QRadar® plug-in, you can access the **Manage Vulnerable Computers** dashboard from the BigFix **Endpoint Protection** domain.

Before installing the QRadar® plug-in, complete the following prerequisite steps as necessary:

- Ensure that the `BES Server Plugin Service` is installed on the BigFix server and is configured correctly.
- Create a new console user for the installation of the QRadar® plug-in and assign `master operator` privileges to that user.
- After you install the `BES Server Plugin Service` on the server, enable encryption of the credentials for the BigFix REST API by running the `Configure REST API credentials for BES Server Plugin Service` Task from **Fixlets and Tasks** node of the **All Content** domain.
  1. Click the `Configure REST API credentials for BES Server Plugin Service` Task. The user interface from which you must start the encryption enablement Task is displayed.
  2. Enter the user name and password for the master operator user that you created. This creates an encrypted password.
  3. Click **Take Action** and specify the server where you are installing the QRadar® plug-in, which is the BigFix server.

 **Note:** The `Configure REST API credentials for BES Server Plugin Service` Task remains relevant after you run it. You can check the action history to confirm that it runs successfully.

- Ensure that the BigFix agent is version 9.2.6 or later is installed on the BigFix server.

To enable QRadar® and BigFix to communicate, you must complete some short configuration steps in QRadar®. For information about how to complete the QRadar® configuration, see the [QRadar and BigFix integration setup](#) wiki. From within BigFix, you must run a Fixlet to install the QRadar® plug-in. This section describes how to install the QRadar® plug-in in BigFix. After you install the plug-in and complete the configuration that

is required in QRadar®, QRadar® posts vulnerability scan data to the BigFix server using the REST API.

Complete the following steps to install the QRadar® plug-in.

1. From the BigFix console, go to the **Endpoint Protection** domain.
2. Click **Manage Vulnerabilities**, then **Setup and Maintenance**, and then **Fixlets and Tasks**.
3. Depending on the operating system on which you are installing the dashboard service, select the `Install or Update the QRadar Plugin on Windows` or `Install or Update the QRadar Plugin on Linux` Fixlet.
4. Review the information in the Fixlet description and if necessary, complete any prerequisite information described.
5. Click **Take Action**. From the **Take Action** dialog box, target the BigFix server.
6. Click **OK** to run the installation Fixlet.

After the Fixlet runs successfully, the dashboard service starts automatically. To open the dashboard on the console, go to the **Endpoint Protection** domain, and click **Manage Vulnerable Computers**.

The plug-in is installed in the following location on the BigFix server:

- On Microsoft™ Windows™ systems, the plug-in is installed in the `C:\Program Files (x86)\BigFix Enterprise\BES Server\Applications\qrplugin` directory.
- On Linux™ systems, the plug-in is installed in the `/var/opt/BESServer/Applications/qrplugin` directory.

## Uninstalling the plugin

A Fixlet is available to uninstall the plugin for the **Manage Vulnerable Computers** dashboard.

To uninstall the **Manage Vulnerable Computers** dashboard, run the uninstallation Fixlet for your platform and target the BigFix server.

1. From the BigFix console, go to the **Endpoint Protection** domain.

2. Click **Manage Vulnerabilities**, then **Setup and Maintenance**, and then select **Fixlets and Tasks**.
3. Depending on the operating system on which you are uninstalling the plugin, select one of the following Fixlets:
  - a. Uninstall the Manage Vulnerabilities Plugin on Windows.
  - b. Uninstall the Manage Vulnerabilities Plugin on Linux.
4. Review the information in the Fixlet description and if necessary, complete any prerequisite information described.
5. Click **Take Action**. From the **Take Action** dialog box, target the BigFix server.
6. Click **OK** to run the uninstallation Fixlet.

# Chapter 2. Remediate vulnerabilities and quarantine computers

Use the **Manage Vulnerable Computers** dashboard to view and remediate QRadar vulnerability data and quarantine or un-quarantine computers.

## Viewing computer details

From the **Manage Vulnerable Computers** dashboard, you can view the computers that you manage in BigFix for which QRadar® sends vulnerability information. You can view the QRadar® Computer Risk Score, number of CVEs, CVE risk score, and quarantine information for each computer. You can filter to view only the computers for which there are relevant Fixlets. You can also quarantine and un-quarantine computers.

The **Computers** tab in the **Manage Vulnerable Computers** dashboard provides you with a view of all the computers that you manage in BigFix for which QRadar® sent vulnerability information. From the **Search** field, you can search for computers. The following graphic shows an example of the **Computers** view. In the computers list, the computers that the BigFix operator manages are displayed. The **QRadar Computer Risk Score** shows the risk assessment for this computer from QRadar®. In this example, the **QRadar Computer Risk Score** is 100, which is a high risk score. The small twistie on **QRadar Computer Risk Score** indicates that the view is sorted by this column. The **CVEs** column shows how many CVEs are impacting this computer as reported by the most recent QRadar® scan that is sent to BigFix. In this example, there are nine CVEs. This view also shows the computer ID, the computer name, operating system, and quarantine status. In the CVEs list, each of the CVEs that are impacting the computer is highlighted. Beside these CVEs, the Fixlet that is available for the currently selected CVE is shown.

In this graphic, the **Show Computers that have Relevant Fixlets** check box is highlighted. By checking this, only computers for which there are relevant Fixlets are displayed and a column is displayed on the dashboard that identifies the number of actionable CVEs for each of the computers. The **Actionable CVEs** column shows the CVEs for which there

are remediation Fixlets available. If you unset this check box, all computers are displayed, including computers for which there are no relevant Fixlets.

**Note:** By design, some Fixlets do not have a default action. If a Fixlet for a CVE does not have a default action, you cannot click **Take Default Action** to run the Fixlet. To run a Fixlet that does not have a default action, click **Open Fixlet**, then click **Take Action**. From the **Take Action** dialog, select an action and target the computers that are impacted by the CVE.

Computer ID	Computer Name	Operating System	Quarantine Status	QRadar Computer Risk Score	Actionable CVEs	CVEs
10067496	SIMULATEDCOMPUTER_9049	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
8861737	NC9098033178	Win2012R2 6.3.9600	Not In Quarantine	100.00	36	100
10054582	SIMULATEDCOMPUTER_160290	Win2012R2 6.3.9600	Not Applicable	100.00	5	100
10099801	SIMULATEDCOMPUTER_160634	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10054784	SIMULATEDCOMPUTER_160986	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10003182	SIMULATEDCOMPUTER_162318	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10023976	SIMULATEDCOMPUTER_163867	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10024842	SIMULATEDCOMPUTER_165233	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10017061	SIMULATEDCOMPUTER_165972	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10020143	SIMULATEDCOMPUTER_166084	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10083957	SIMULATEDCOMPUTER_167745	Win2012R2 6.3.9600	Not Applicable	100.00	5	100
10067496	SIMULATEDCOMPUTER_166130	Win2012R2 6.3.9600	Not Applicable	100.00	4	100

  

CVE ID	CVSS Risk Score
2015-6161	1.00
2015-0008	1.00
2014-3566	1.00
2014-0160	1.00

  

Fixlet ID	Fixlet Name	Site Name	Content Type
1512461	3125869: Vulnerability in Internet Explorer could lead to ASLR bypass - Enable the User32 Exception Handler Hardening	Patches for Windows	Fixlet

Complete the following steps to view computer details.

- From the **Manage Vulnerable Computers** dashboard, click the **Computers** tab.
- Before you can access the complete functionality of the **Computers** tab for the first time, you must activate an analysis. Run the analysis if prompted. From the **QRadar Computer Risk Score** column, you can view the QRadar® risk assessment for this computer. The **CVEs** column shows how many CVEs are impacting the currently selected computer.
- To display only the computers for which there are relevant Fixlets, check the **Show Computers that have Relevant Fixlets** button. When you check this box, the total

number of computers is reduced to show only computers for which there are relevant computers. If you do not check this box, all computers are listed.

4. To search for a specific computer, enter search criteria in the **Search** field.
5. To remediate a CVE for a computer:
  - a. Select the computer for which you want to remediate a CVE.
  - b. Select a CVE for the computer on the bottom left of the screen.
  - c. From the **Relevant Fixlets** tab, select a relevant Fixlet.
  - d. Click **Take Default Action** to run the Fixlet to remediate the CVE.

## Quarantining computers

You can quarantine Microsoft Windows computers from the **Manage Vulnerable Computers** dashboard.

You must have the policy action set up for quarantining, as described in the [Requirements \(on page 3\)](#) section.

The **Computers** tab in the **Manage Vulnerable Computers** dashboard provides you with a view of all the computers that you manage as a BigFix operator. You can view the computer ID, the computer name, risk scores, quarantine state, and the CVEs associated with computers. You can also quarantine computers.

You can only quarantine one computer at a time. To quarantine a computer, you run a Fixlet that identifies that computer to be quarantined. This computer is then quarantined by the quarantine policy action Fixlet that continuously enforces the policy.

The screenshot shows a table with the following data:

Computer ID	Computer Name	Operating System	Quarantine Status	QRadar Computer Risk Score	Actionable CVEs	CVEs
8861737	NC9098033178	Win2012R2 6.3.9600	Not In Quarantine	100.00	36	100
10054582	SIMULATEDCOMPUTER_160290	Win2012R2 6.3.9600	Not Applicable	100.00	5	100
10099801	SIMULATEDCOMPUTER_160634	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10054784	SIMULATEDCOMPUTER_160986	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10003182	SIMULATEDCOMPUTER_162318	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10023976	SIMULATEDCOMPUTER_163867	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10024842	SIMULATEDCOMPUTER_165233	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10017061	SIMULATEDCOMPUTER_165972	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10020143	SIMULATEDCOMPUTER_166084	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10083957	SIMULATEDCOMPUTER_167745	Win2012R2 6.3.9600	Not Applicable	100.00	5	100
10062029	SIMULATEDCOMPUTER_168139	Win2012R2 6.3.9600	Not Applicable	100.00	4	100
10000000	SIMULATEDCOMPUTER_170007	Win2012R2 6.3.9600	Not Available	100.00	4	100

The quarantine and un-quarantine feature is available only for Microsoft Windows computers.

Complete the following steps to quarantine a Microsoft Windows computer.

- From the **Manage Vulnerable Computers** dashboard, click the **Computers** tab. From the **CVEs** and **QRadar Computer Risk Score** columns, you can view the number of CVEs and risk scores associated with the computers. In particular, the **QRadar Computer Risk Score** column provides enriched risk assessment data from QRadar® and identifies the computers that are most at risk.
- Select a Microsoft Windows computer that you want to quarantine.
- Click **Quarantine Computer**. If your BigFix console version is an earlier version than version 9.2.6, all computers are loaded in the **Take Action** screen, rather than the computer that you selected in the previous step. If you want to load only the computer that you select in the previous step, upgrade your console to version 9.2.6 or later before proceeding.
- From the **Take Action** dialog, select the computer. From the **Execution** tab, you can schedule a time and date for the quarantine.
- Click **OK** to quarantine the computer. After this action completes, the policy action Fixlet detects that the computer needs to be quarantined and quarantines the computer. It might take some time before the status of the computer is changed to **Quarantined** on the dashboard. Click the **Refresh** icon to refresh the data if the **Quarantine Status** is slow to update.

Only one action is generated for the quarantine Fixlet. So for each subsequent computer that you quarantine, the existing quarantine action is updated to include the latest computer quarantined. To view an updated action, from the **Endpoint Protection** domain, select **Actions** and select the **Quarantine** action. Click **Reported Computers** and you can see the computers for which the quarantine action has run.

## Un-quarantining computers

From the **Manage Vulnerable Computers** dashboard you can view all of the computers that you manage in BigFix and view CVEs, associated risk, and quarantine data for each computer. You can also quarantine and un-quarantine Microsoft Windows computers.

You must have the policy action set up for un-quarantining, as described in the [Requirements \(on page 3\)](#) section.

You can view the computer ID, the computer name, QRadar Computer Risk Score, quarantine state, and CVEs associated with the computers that you manage. Using this enriched vulnerability information, you can quickly identify the computers that are at risk. You can also quarantine and un-quarantine computers.

You can un-quarantine only Microsoft Windows computers and you can un-quarantine only one computer at a time.

Complete the following steps to un-quarantine a Microsoft Windows computer.

1. From the **Manage Vulnerable Computers** dashboard, click the **Computers** tab.
2. Select the computer that you want to un-quarantine.
3. Click **Un-quarantine Computer**.
4. From **Execution** tab on the **Take Action** dialog box, you can schedule a time for the computer to be un-quarantined, or click **OK** to un-quarantine the computer immediately.

Only one action is generated for the un-quarantine Fixlet. So for each subsequent computer that you un-quarantine, the existing un-quarantine action is updated to include the latest computer un-quarantined. To view an updated action, from the **Endpoint Protection** domain,

select **Actions** and select the `Un-quarantine` action. Click **Reported Computers** and you can see the computers for which the un-quarantine action has run.

## Viewing Common Vulnerability Exposures (CVEs) and associated Fixlets

The **Manage Vulnerable Computers** dashboard displays vulnerability data from QRadar®. The vulnerabilities detected by QRadar® are known as Common Vulnerability Exposures (CVEs). This CVE data is displayed in the dashboard for the computers that you control as an operator in BigFix. The **Manage Vulnerable Computers** dashboard does not display all CVEs detected for all computers by QRadar® Vulnerability Manager. Only CVEs with a risk score above a threshold defined in QRadar® are sent to the **Manage Vulnerable Computers** dashboard.

From the **Manage Vulnerable Computers** dashboard, you can view a list of CVEs for the computers that you manage. You can also view the BigFix Fixlets, including any superseded Fixlets, that are available to remediate any particular CVE. Fixlets are the BigFix actions that remediate or fix vulnerabilities. You can also filter to view only the CVEs for which there are relevant Fixlets.

BigFix provides a large number of Fixlets to patch endpoints and remediate vulnerabilities. For example, the BigFix patch sites contain Fixlets for different operating systems and application patches. For any particular computer to evaluate whether or not a Fixlet is relevant, the computer must be subscribed to the site that contains the Fixlets. For many CVEs, there are Fixlets available to remediate the CVEs. For some CVEs, there might be one or more Fixlets available. By selecting a CVE, you can view any applicable Fixlets for the CVE.

The following graphic shows an example of the CVEs view. The list of CVEs is filtered to show only the CVEs for which there are relevant Fixlets.

Manage Vulnerable Computers

Filter to show only the CVEs for which there are relevant Fixlets

Shows the number of computers that impacted by the CVE and for which there is remediation content

Nov 24, 2016 3:46:35 AM

**CVEs**   **Computers**

92 Common Vulnerabilities and Exposures

Show CVEs that have Relevant Fixlets   Refresh

Search

CVE ID	CVSS Risk Score	Impacted Computers	Actionable Impacted Computers
2016-7253	1.00	1022	1
2016-7254	1.00	1022	1
2016-S290	1.00	1022	2
2016-S289	1.00	1022	2
2016-9071	1.00	1022	2
2016-9063	1.00	1022	2
2016-9076	1.00	1022	2
2016-9074	1.00	1022	2
2016-9073	1.00	1022	2
2016-9070	1.00	1022	2
2016-9062	1.00	1022	2

**Relevant Fixlets**   **Computers**   **Action History**

1 Relevant Fixlets for 2016-7253

Search

Fixlet ID	Fixlet Name	Site Name	Applicable Computers	Associated Actions	Content Type
1613623	MS16-136: Security Update for SQL Server - SQL Server 2012 SP3 - GDR Branch - KB3194721 (x64)	Patches for Windows	1	0	Fixlet

[Open Fixlet](#)   [Take Default Action](#)

 **Important:** Some CVE data displayed on the **Manage Vulnerable Computers** dashboard might be slightly out of date until new scan data is received from QRadar®. For example, if you run a Fixlet that remediates a CVE, the CVE is not removed from the dashboard until a new scan is received from QRadar®.

Complete the following steps to view CVEs and applicable Fixlets that are available for a CVE.

1. From the **Manage Vulnerable Computers** dashboard, click the **CVEs** tab. The list of CVE data from QRadar® for the computers that you manage in BigFix is displayed.
  2. Select a CVE. Any available Fixlets to correct the CVE are loaded.

A Fixlet might not have been developed for the particular CVE.

### Scenario 2

A Fixlet or Fixlets might already have been run to remediate the CVE, and there are no remaining relevant Fixlets.

### **Scenario 3**

A Fixlet is available for the CVE, but computers are not subscribed to the site that contains the Fixlet. For Fixlets to be evaluated by computers, the computers must be subscribed to the site. The site must be enabled and the contents must be gathered.

### **Scenario 4**

A Fixlet is available for the CVE, but as an operator, you might not be subscribed to the site that contains the Fixlet. If you are not subscribed to the site that contains the Fixlet, the Fixlet is not displayed.

### **Scenario 5**

A Fixlet is available for the CVE, but it might not be applicable to some computers. The CVE might have been remediated, rendering the Fixlet not relevant on that computer. For example, an operator might have remediated the specific CVE, or an application might have been removed, an application or operating system might have been upgraded. The **Actions** tab might indicate if a Fixlet was previously run for the CVE.

### **Scenario 6**

In exceptional circumstances, a Fixlet might have been archived by HCL. Typically if a Fixlet has been archived, another Fixlet is available that supersedes it, and the superseded Fixlet is typically available.

3. To view only CVEs for which there are relevant Fixlets, check the **Show CVEs that have Relevant Fixlets** check box.
  
4. Click **Open Fixlet** to view the source Fixlet or click **Take Default Action** to run the Fixlet to remediate the CVE. If you want to schedule the Fixlet to run during a patch window, click the **Execution** tab and select the time and date that you want the Fixlet to run. Then click **Submit** to run the action. To view the processing status for actions, click the **Actions** tab.

## Viewing actions

From the **Actions** tab on the **Computers** or **CVEs** view, you can track the progress of actions that you deployed from the **Manage Vulnerable Computers** dashboard.

From the dashboard, you can view the actions that you deployed to run Fixlets and superseded Fixlets. An **Actions** tab is available from within both the **CVEs** view and the **Computers** view. Actions for the quarantine and un-quarantine Fixlets are not shown on the **Actions** tab.

Complete the following steps to track the progress of actions that you deployed from the **CVEs** or **Computers** view.

1. From the **Manage Vulnerable Computers** dashboard, click the **CVEs** or **Computers** tab.
2. Click the **Actions** tab.
3. Select an action to view detailed information about the action execution.

## Common problems and troubleshooting

Read this section for information about any known issues using the **Manage Vulnerable Computers** dashboard.

For more information about the **Manage Vulnerable Computers** dashboard, see the [BigFix wiki](#).

To help troubleshoot issues that you might experience using the **Manage Vulnerable Computers** dashboard, review the following troubleshooting tips:

### Verify that the installation is successful

Check that the action for the `Install` or `Update the Manage Vulnerabilities Plugin` completed successfully and make sure that the Fixlet is no longer relevant. Allow some time for the action to complete and for the relevance to be evaluated.

## Checking for data posted by QRadar®

To check for incoming data from QRadar®, check the dashboard variable under which QRadar® posts data on the BigFix server. On the BigFix server, open the following URL in a browser and log in using your BigFix credentials: <https://127.0.0.1:52311/api/dashboardvariables/QRadarScan.ojo>.

Every time that QRadar® sends data to your BigFix server, a unique variable is created under `QRadarScan.ojo`. If there are no variables or `QRadarScan.ojo` does not exist, QRadar® has not sent any data to the BigFix server. The variable name starts with the date on which the scan was run, for example:

```
<Value>{"name": "20160118.120854.285.1 QRadar Data", "assets": [
    {"fqdn": "SIWW14EMMX-014", "besid": "251301", "cves": [
        {"id": "2015-6112", "risk": 1},
        {"id": "2015-6113", "risk": 1},
        {"id": "2015-6104", "risk": 1},
        {"id": "2015-6103", "risk": 1}, {"id": "2015-6102", "risk": 1}, {"id": "2015-6101", "risk": 1}
    ]
}
```

In addition, `besid` identifies the BigFix computers to which the CVE information relates.

## No BigFix content appearing for CVE or computer

Make sure that you have permission to manage the computers as an operator in BigFix. Operators see only the computers in BigFix for which they have permission to manage. For more information, see: [https://help.hcltechsw.com/bigfix/9.5/platform/Platform/Console/c\\_operators.html](https://help.hcltechsw.com/bigfix/9.5/platform/Platform/Console/c_operators.html).

Make sure that you have access to the site. As an operator, you must also have access to the site. For more information, see: [https://help.hcltechsw.com/bigfix/9.5/platform/Platform/Console/c\\_operators.html](https://help.hcltechsw.com/bigfix/9.5/platform/Platform/Console/c_operators.html).

Make sure that the computers are subscribed to the patch sites that contain the remediation content. Computers must be subscribed to relevant patch sites for content to be available, otherwise the filter eliminates them from the original data set because they have no relevant content. For more

information, see: [https://help.hcltechsw.com/bigfix/9.5/platform/Platform/Console/c\\_viewing\\_site\\_properties.html?hl=viewing%2Csite%2Cproperties](https://help.hcltechsw.com/bigfix/9.5/platform/Platform/Console/c_viewing_site_properties.html?hl=viewing%2Csite%2Cproperties).

### **Checking that the QRadar® process is running**

To check if the QRadar® process is running, check the processes on the **Task Manager**. When the QRadar® plugin is installed and running, the `QRadarNode.exe` process is visible from the **Task Manager**.

### **Logging**

The log files for the QRadar® plugin are located in the `C:\Program Files\Bigfix Enterprise\BES Server\Applications\Logs` directory.

### **No Fixlet for CVE**

For complete information, see [Viewing Common Vulnerability Exposures \(CVEs\) and associated Fixlets \(on page 14\)](#).

### **Unable to quarantine or un-quarantine computers**

If you are unable to successfully quarantine or un-quarantine Microsoft Windows computers, make sure that the policy actions are set up correctly for the quarantine or un-quarantine Fixlets. See the [Requirements \(on page 3\)](#) for more information.

# Chapter 3. Support

For more information about this product, see the following resources:

- [Knowledge Center](#)
- [BigFix Support Center](#)
- [BigFix Support Portal](#)
- [BigFix Developer](#)
- [BigFix Wiki](#)
- [HCL BigFix Forum](#)

# 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.