

BigFix Insights for Vulnerability Remediation Implementation Guide



Special notice

Before using this information and the product it supports, read the information in [Notices \(on page 65\)](#).

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.....	1
Chapter 2. System requirements.....	3
Chapter 3. Deployment and configuration.....	8
Chapter 4. Advanced Configuration.....	11
Chapter 5. Business Intelligence reports.....	13
Chapter 6. Reference.....	35
Configuration file.....	35
Configuration settings for IVR solution.....	41
Command line interface.....	46
Logs.....	47
Troubleshooting.....	48
Known limitations.....	49
Appendix A. Glossary.....	51
Notices.....	65
Index.....	

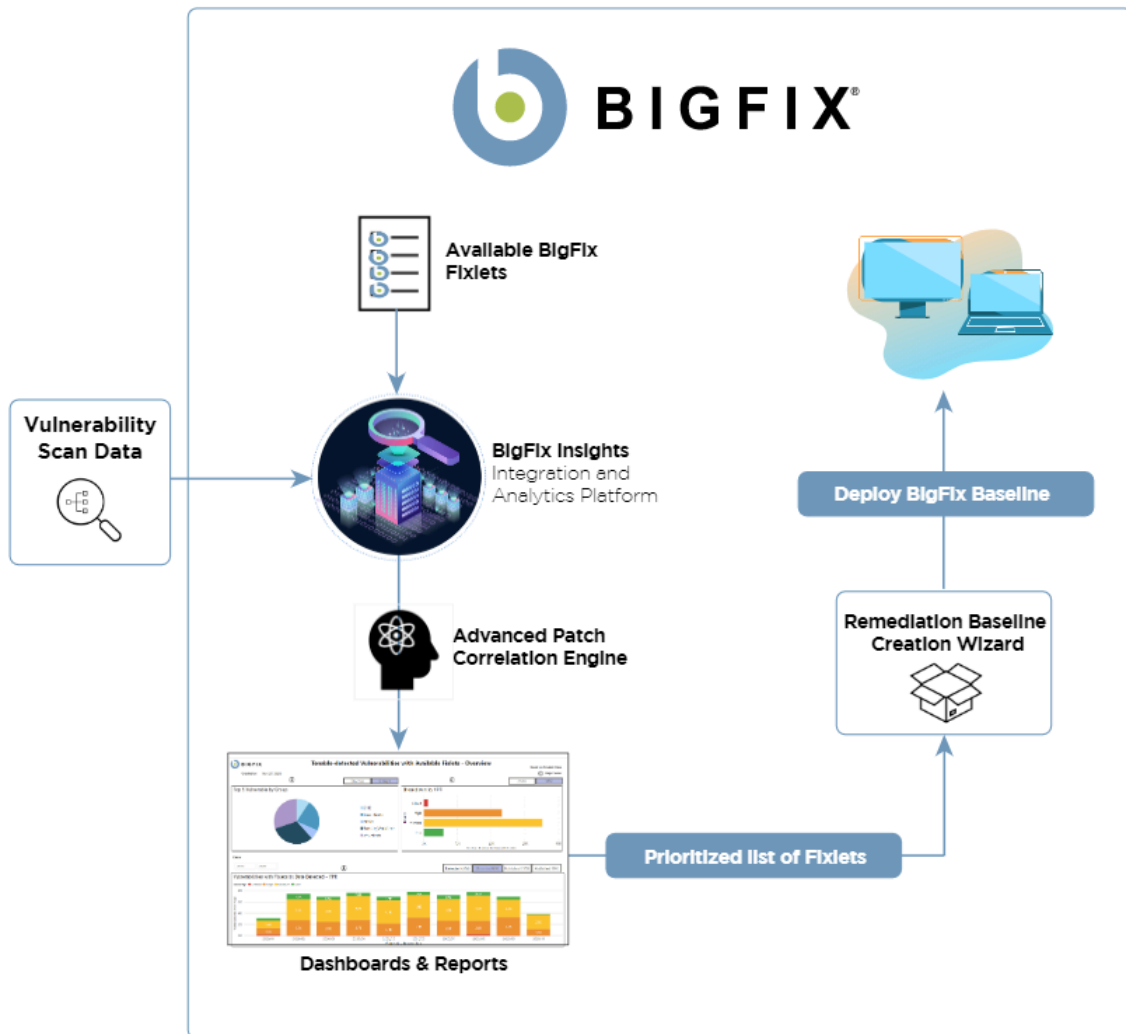
Chapter 1. BigFix Insights for Vulnerability Remediation

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.

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. The table below describes prerequisites and system requirements for IVR service.

Hardware requirements	
CPU	minimum 2 cores (recommended 4)
RAM	On top of host OS requiremenst: • < 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

Table 1. The table below describes prerequisites and system requirements for IVR service. (continued)

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	
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
Operating system	• Microsoft Windows 2016 • Microsoft Windows 2019
Supported BigFix versions	• Windows - based BigFix Server, Version 10  Note: BigFix Insights for Vulnerability Remediation

Table 1. The table below describes prerequisites and system requirements for IVR service. (continued)

	 does not currently support non-Windows-based BigFix Server environments.
BigFix Component Requirements	• BigFix Insights
BigFix License Requirements	• BigFix Lifecycle • BigFix Compliance
Supported Vulnerability Management Platforms	• Qualys VMDR v2 REST API: https://www.qualys.com/docs/qualys-api-vmqc-user-guide.pdf • Tenable.SC
BI tool	• Power BI Desktop/Server, 2019 + (Rec. May 2020)  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 +

Table 1. The table below describes prerequisites and system requirements for IVR service. (continued)

Network requirements	• Connectivity to Vulnerability Management API Server URL (port 443 by default) • Connectivity to BigFix Insights SQL database (port 1433 by default)
-----------------------------	--

Vulnerability Management API details

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 (on
page 41) ) + (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.

Tenable API requirements

The IVR server requires a Tenable user account. A user leveraged to Tenable.sclVR 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.

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.

Chapter 3. Deployment and configuration

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:

1. Run installation command

Purpose: This step installs the BFIVR (BigFix Insights for Vulnerability Remediation) executable as a windows service.

- a. Navigate to the installation directory and run **BFIVR.exe --Install** command.

When successful, the message *'Installing service BFIVR. Service installed.'* appears in the command prompt.

2. Define the target for BigFix Insights

Purpose: This step defines how the dataflow targets the Insights database.

- a. Note down of the Insights Server IP and the database name.
- b. Create a connection string.
- c. Navigate to the installation directory and run **BFIVR.exe --UpdateTargetURL BigfixINSIGHT "<Your_ODBC_String>"** command.



Important: The ODBC string must be written within double quotes.

3. Define the target for the scanner

Purpose: This step defines how the dataflow targets the scanner URL.

- a. Take a note of the Tenable.sc scanner IP and port
- b. Navigate to the installation directory and run **BFIVR.exe --UpdateTargetURL TenableSC https://<Server>:<Port>** command.

If the IP of the Tenable Server is 192.168.0.133 and the target port is the default https port, the command looks as: `C:\BFIVR\BFIVR.exe -- UpdateTargetURL TenableSC https://192.168.0.133`. To confirm the command, verify the `DataflowsConfig.xml` file in the installation path. The file should now reference the parameters that you have defined as connection string for the Tenable sc datasource.

4. Set the credentials for Insights

Purpose: This step defines how the dataflow authenticates with the Big Fix Insights database for standard ETL (Expand, Transform, Load) operations.

- a. Obtain the credentials for your BigFix Insights database.
- b. Navigate to the installation directory and run `\BFIVR.exe -- ProvideCredentials BigfixINSIGHT -Creds <Insights_User> <Insights_Pass>` command.



Note: The database writer must have access to the account in BigFix Insights database.

Example: If the username is 'insights' and the associated password is 'BigFix123', the command looks as: `'C:\BFIVR\BFIVR.exe -- ProvideCredentials BigfixINSIGHT -Creds insights BigFix123`. When successful, the message 'The credentials provided are encrypted successfully!' appears in the command prompt.

5. Set the credentials for the scanner

Purpose: This step defines how the dataflow authenticates with the Tenable.sc scanner.

- a. Obtain the credentials for your Tenable.sc server.
- b. Navigate to the installation directory and run `\BFIVR.exe -- ProvideCredentials TenableSC -Creds <TenableSC_User> <TenableSC_Pass>` command.

Example: If the username is 'secmanager' and the associated password is 'BigFix123', the command looks as:
`C:\BFIVR\BFIVR.exe -- ProvideCredentials TenableSC -Creds secmanager BigFix123.`

When successful, the message *'The credentials provided are encrypted successfully!'* appears in the command prompt.

6. Initialize the IVR schema on Insights

Purpose: This step defines initializes the IVR Schema within BFInsights.

- a. Obtain the credentials for your BigFix Insights database.
- b. Navigate to the installation directory and run `\BFIVR.exe -- ProvideCredentials --InitializeSchemas -Creds <Insights_User> <Insights_Pass>` command.



Note: The account should have DBO rights to the database BigFix Insights DB.

Example: If the username is insights and the associated password is BigFix123, the command looks as follows:

`C:\BFIVR>BFIVR.exe --InitializeSchemas -Creds insights BigFix123.` When successful, the message *'Schema Initialized Successfully!'* appears in the command prompt.

7. Validate the configuration

Purpose: This step verifies the configuration provided from the previous steps.

- a. Navigate to the installation directory and run `\BFIVR.exe -- ValidateConfiguration` command.

When successful, the message *'Configuration verified successfully!'* appears in the command prompt.

Chapter 4. Advanced Configuration

Learn how to update and validate configuration.

Updating the configuration

To update the configuration file, perform these steps:

1. Log in to the target server.
2. Navigate to the project installation directory.
3. Open the `DataFlowsConfig.xml` file in your preferred text editor.
4. Update configuration. For more information, refer to [Configuration Settings \(on page 41\)](#).
5. Save the changes.

Validating the configuration

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.

Updating the credentials

To update the credentials, perform these steps:

1. Open CLI and run the `BFIVR.exe --ProvideCredentials` command.
You are prompted to enter a username and password.
2. Enter login credentials for the data source:
 - Username
 - Password

On successful update, the message, *The entered credentials are encrypted successfully.* appears in the command prompt.



Note: Any changes to the configuration file purges all IVR data associated with the current dataflow configuration (from which we generate a hash), as well as all data not associated with existing dataflow configurations. For more information, refer to [PurgeFindingsOnExecutionOfDataflow \(on page 41\)](#) setting.

Chapter 5. 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

- 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 portayed on the Dashoboard page. Vizualizations that do not apply to your business process can be removed as necessary.

Qualys

- **Vulnerabilities with Available Fixlets**

Figure 2. Detected Vulnerable Devices with Applicable Fixlets – Overview

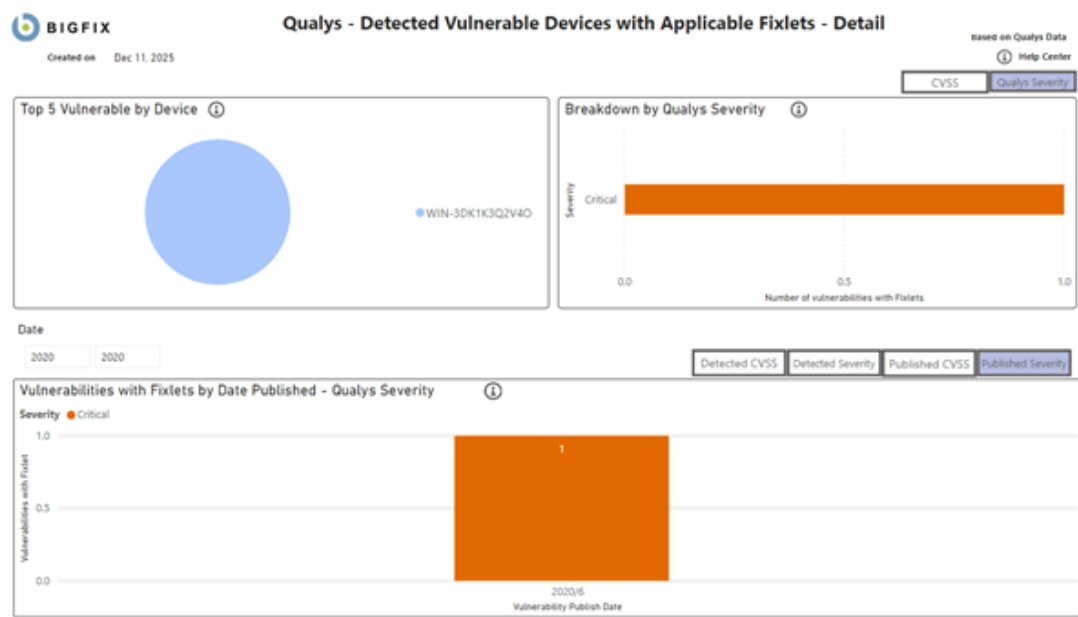


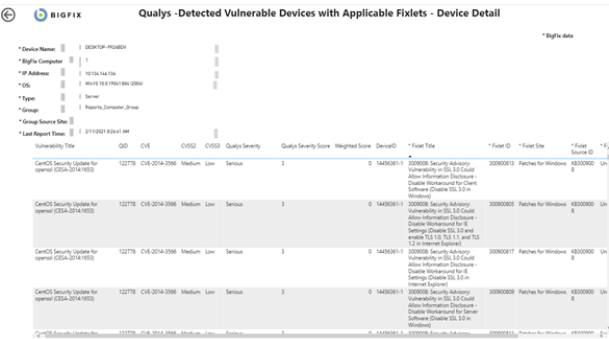
Figure 2. Detected Vulnerable Devices with Applicable Fixlets – Vulnerability List

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)	CVS-2020-1108	238356	Low	High	Critical	4	3	6/15/2020	6/16/2020	1	Windows

Figure 2. Detected Vulnerable Devices with Applicable Fixlets – Device Vulnerabilities



Figure 2. Detected Vulnerable Devices with Applicable Fixlets – Device Detail



• Vulnerabilities without Available Fixlets

Tenable

Vulnerabilities with Available Fixlets

Figure 6. Detected Vulnerable Devices With Applicable Fixlets - Overview

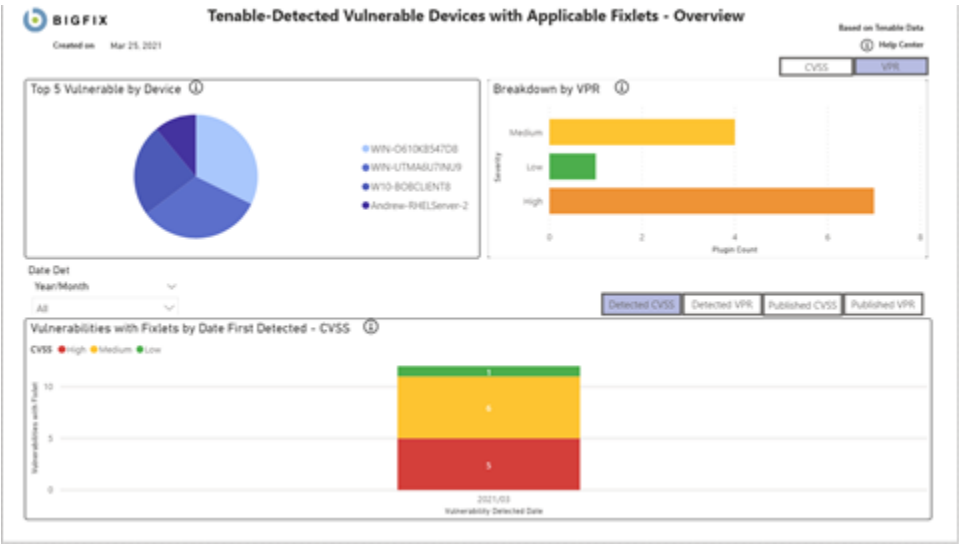


Figure 6. Detected Vulnerable Devices With Applicable Fixlets - Vulnerability List

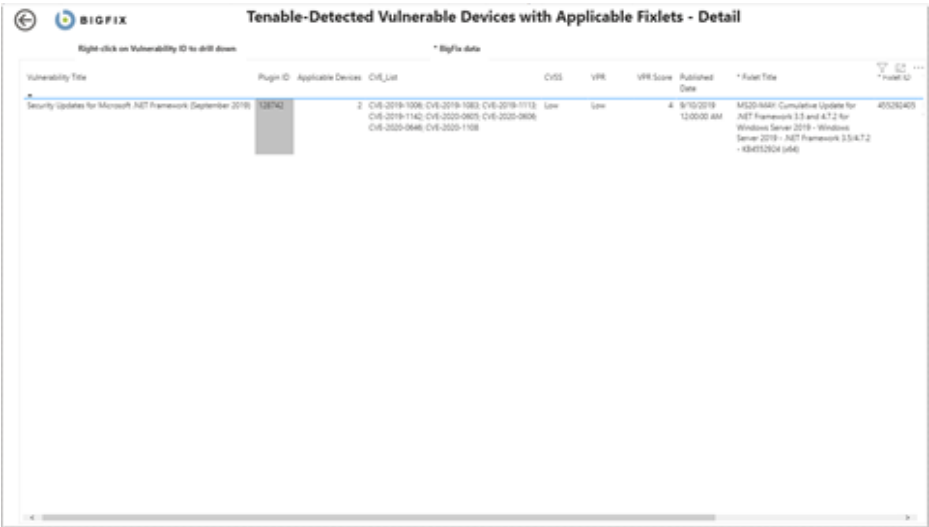
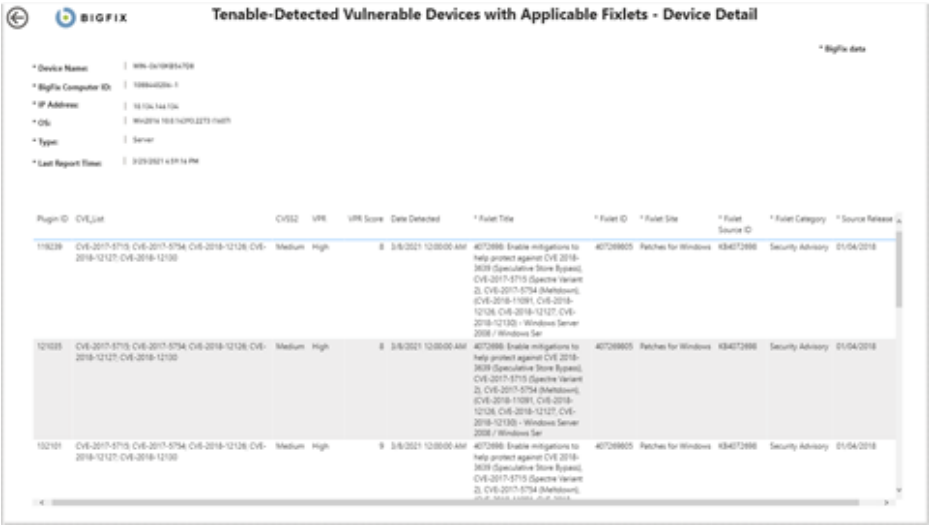


Figure 7. Detected Vulnerable Devices with Applicable Fixlets - Vulnerability Detail



Figure 8. Detected Vulnerable Devices With Applicable Fixlets - Device Detail



• Vulnerabilities without Available Fixlets

Figure 8. Detected Vulnerable Device without Applicable Fixlets - Overview

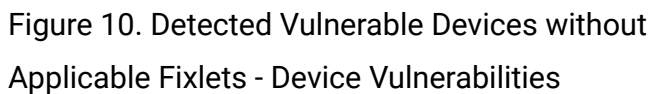
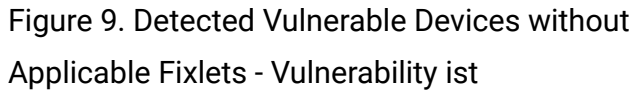




Figure 12. Detected Vulnerability Discrepancies – Vulnerability List

Vulnerability Title	Plugin ID	CVE ID	CVSS	Severity	VMs	Applicable Devices	Published Date	Fixed Date	Fixed Title	Fixed Date	Fixed Title	Fixed Date
MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	1000000	CVE-2020-1018	High	Critical	10	1	4/10/2020	4/10/2020	MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	4/10/2020	MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	4/10/2020
MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	1000000	CVE-2020-1019	High	Critical	10	1	4/10/2020	4/10/2020	MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	4/10/2020	MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	4/10/2020
MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	1000000	CVE-2020-1020	High	Critical	10	1	4/10/2020	4/10/2020	MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	4/10/2020	MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	4/10/2020

Figure 12. Detected Vulnerability Discrepancies – Device Vulnerabilities

Vulnerability Title	Plugin ID	CVE ID	CVSS	Severity	VMs	Applicable Devices	Published Date	Fixed Date	Fixed Title	Fixed Date	Fixed Title	Fixed Date
MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	1000000	CVE-2020-1018	High	Critical	10	1	4/10/2020	4/10/2020	MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	4/10/2020	MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	4/10/2020

Figure 12. Detected Vulnerability Discrepancies – Device Detail

Device Name	IP Address	Severity	CVSS	Published Date	Fixed Date	Fixed Title	Fixed Date
Device 1	10.10.10.10	High	Critical	4/10/2020	4/10/2020	MS00-021: Windows 10 Windows 10 and Windows Server 2019 April 2020 Security Update	4/10/2020

Tableau reports

- 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 portayed on the Dashboard page. Vizualizations that do not apply to your business process can be removed as necessary.

Qualys

Vulnerabilities with Available Fixlets

Figure 18. Detected Vulnerable Devices With Applicable Fixlets - Overview

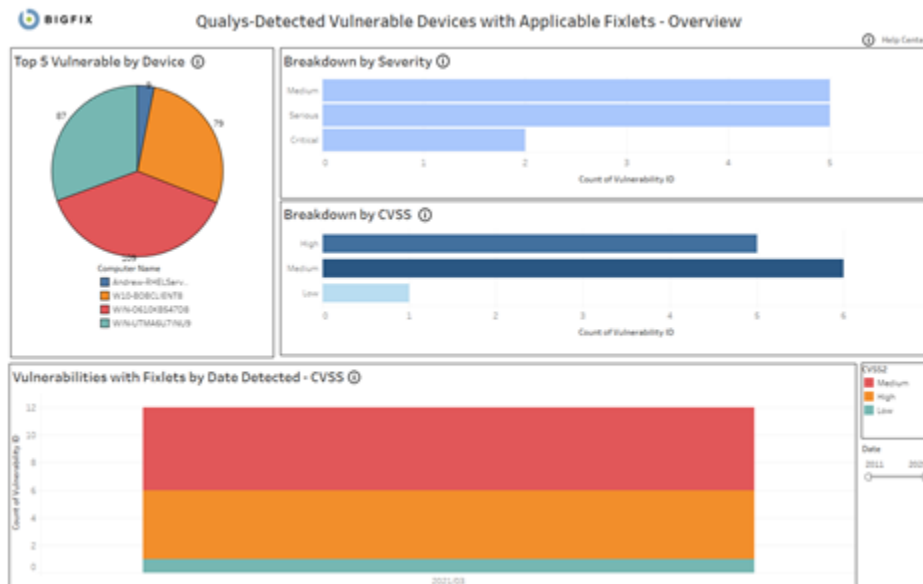


Figure 18. Detected Vulnerable Devices With Applicable Fixlets - Overview



Figure 19. Detected Vulnerable Devices With Applicable Fixlets - Vulnerability List

BIGFIX

Right-click on Vulnerability ID to drill down

Qualys-Detected Vulnerability List - Detail

Vulnerability Title	Vulnerability - CVE List	CVSS2	Severity	Applicable...	Year of Pub.	* Fixlet Title	* Fixlet ID	* Fixlet Sec.	* Fixlet Site
Adobe Flash Player v32.0.0.137263	CVE-2020-8767, CVE-2020-9633	high	Critical	2	2020	MS20-OCT: Security update for Adobe Flash	458032525	KB4580325	Patches for...
KB4587759: Security update...	137263	high	Serious	2	2020	MS20-OCT: Security update for Adobe Flash	458032525	KB4580325	Patches for...
KB4581863: Windows 10 Win...	138463	high	Serious	3	2020	MS20-NOV: Cumulative update for .NET 4...	458203405	KB4580441	Patches for...
KB4589990: Windows 10 Win...	138463	high	Serious	3	2020	MS21-APR: Servicing Stack Update for Wi...	500089011	KB5000889	Patches for...
Security Updates for Windows...	137999	high	Critical	2	2020	MS20-NOV: Cumulative update for .NET 4...	458203405	KB4580441	Patches for...

Figure 20. Detected Vulnerable Devices With Applicable Fixlets - Device Vulnerabilities

BIGFIX

Right-click on Device ID to drill down

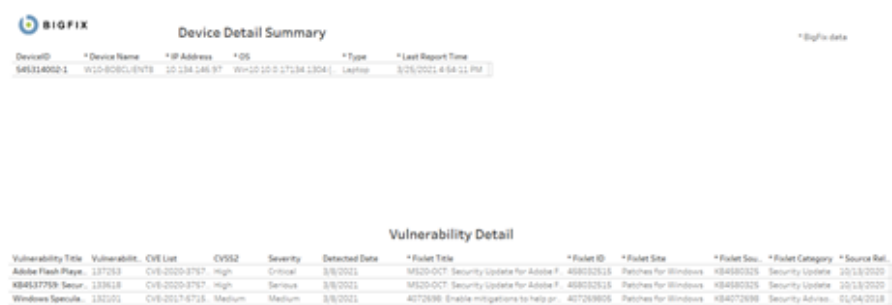
Vulnerability Device Summary

Vulnerability	Vulnerability - CVE List	Year of Pub.	CVSS2	Severity	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sec.	* Fixlet Category	* Source Release De...
Adobe Flash	137263	2020	high	Critical	MS20-OCT: Security update for Adobe Flash Player v...	458032525	Patches for Windows	KB4580325	Security update	20/10/2020

Vulnerability Device Detail

Detected Date	DeviceID	* Device Name	* OS	* IP Address	* Type	* Last Report Time
8/9/2021	10373210-5	WIN-VTMM6U7N9	WIN-2019 10.0.17763.1071	172.17.128.1	Server	8/9/2021 4:57:12 PM
	545314002-5	WIN-8080L6N78	WIN-2019 10.0.17134.1304 (S)	10.134.146.97	Laptop	8/9/2021 4:54:11 PM

Figure 21. Detected Vulnerable Devices With Applicable Fixlets - Device Detail



Vulnerabilities without Available Fixlets

Figure 21. Detected Vulnerable Devices Without Applicable Fixlets - Overview

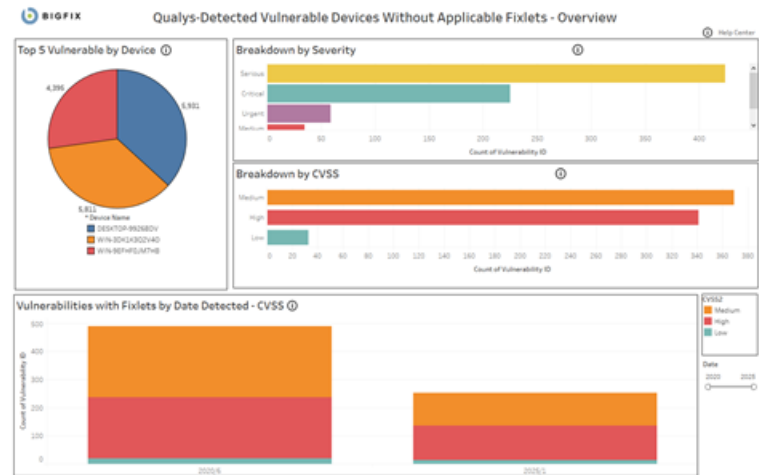


Figure 22. Detected Vulnerable Devices Without Applicable Fixlets - Overview





Figure 25. Detected Vulnerable Devices Without Applicable Fixlets - Device Detail



Vulnerability Discrepancies

Figure 26. Detected Vulnerability Discrepancies - Overview

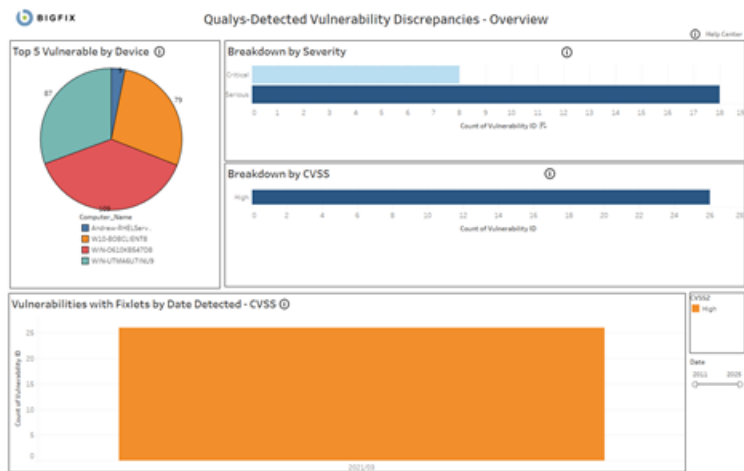


Figure 26. Detected Vulnerability Discrepancies - Overview



Figure 27. Detected Vulnerability Discrepancies - Vulnerability List

Qualys-Detected Vulnerability Discrepancies - Detail											
Vulnerability	Vulnerability ID	CVE ID	CVSS2	Severity	Application	Year of Pub.	* Fixlet Title	* Fixlet ID	* Fixlet Desc.	* Fixlet Site	* Fixlet Category * Source Ref.
MS00-0001	144500	CVE-2020-0-0	high	Critical	0	2020	MS00-0001 Cumulative Update for Windows	000000001	000000001	Patches for Windows	Security Update 10/19/2023
MS00-0002	144501	CVE-2020-0-0	high	Critical	0	2020	MS00-0002 Cumulative Update for Windows	000000002	000000002	Patches for Windows	Security Update 10/19/2023
MS00-0003	144502	CVE-2020-0-0	high	Critical	0	2020	MS00-0003 Cumulative Update for Windows	000000003	000000003	Patches for Windows	Security Update 10/19/2023
MS00-0004	144503	CVE-2020-0-0	high	Critical	0	2020	MS00-0004 Cumulative Update for Windows	000000004	000000004	Patches for Windows	Security Update 10/19/2023
MS00-0005	144504	CVE-2020-0-0	high	Critical	0	2020	MS00-0005 Cumulative Update for Windows	000000005	000000005	Patches for Windows	Security Update 10/19/2023
MS00-0006	144505	CVE-2020-0-0	high	Critical	0	2020	MS00-0006 Cumulative Update for Windows	000000006	000000006	Patches for Windows	Security Update 10/19/2023
MS00-0007	144506	CVE-2020-0-0	high	Critical	0	2020	MS00-0007 Cumulative Update for Windows	000000007	000000007	Patches for Windows	Security Update 10/19/2023
MS00-0008	144507	CVE-2020-0-0	high	Critical	0	2020	MS00-0008 Cumulative Update for Windows	000000008	000000008	Patches for Windows	Security Update 10/19/2023
MS00-0009	144508	CVE-2020-0-0	high	Critical	0	2020	MS00-0009 Cumulative Update for Windows	000000009	000000009	Patches for Windows	Security Update 10/19/2023
MS00-0010	144509	CVE-2020-0-0	high	Critical	0	2020	MS00-0010 Cumulative Update for Windows	000000010	000000010	Patches for Windows	Security Update 10/19/2023

Figure 28. Detected Vulnerability
Discrepancies - Device Vulnerabilities

Qualys-Detected Vulnerability Discrepancies - Device Summary

Right-click to download

Year of Risk	CVE	Severity	Faked Risk	Faked Score	Faked Status	Faked Category
01/01/2020	CVE-2020-0446	Critical	100.0	10.0	Not Patches for Windows	Security (Legacy)

Right-click on Device ID to drill down

Qualys-Detected Vulnerability Discrepancies - Device Detail

Device ID	DeviceID	Computer Name	OS	IP Address	Type	Last Report Time
104561601	104561601	WIN7-PRO-PC	Windows 7	192.168.1.100	Server	2020-01-01 10:00:00

Figure 29. Detected Vulnerability Discrepancies - Device Detail

[illegible]

Tenable

Vulnerabilities with Available Fixlets

Figure 33. Detected Vulnerable Device with Applicable Fixlets - Overview

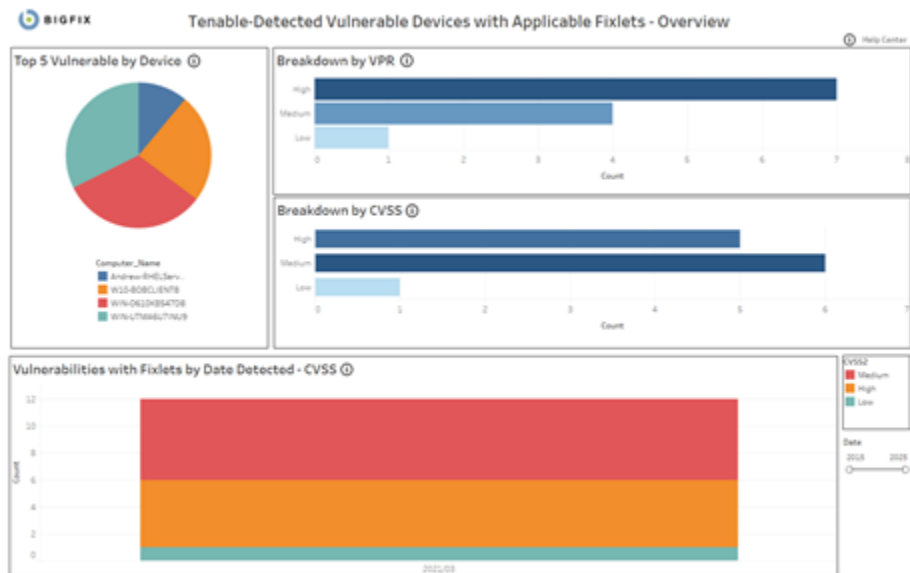


Figure 34. Detected Vulnerable Devices with Applicable Fixlets - Overview



Figure 34. Detected Vulnerable Devices with Applicable Fixlets - Vulnerability List

 **Tenable-Detected Vulnerability List - Detail** * BigFix data

Right-click on Plugin ID to drill down

Vulnerability	Plugin 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...	468032515	KB4580325	Patches for Windows	Security Update	10/13/2020
KB4537759	138618	CVE-2020-3757	High	Medium	2	2020	MS20-OCT: Security Update for A...	468032515	KB4580325	Patches for Windows	Security Update	10/13/2020
KB4518553	138601	CVE-2019-1206	High	High	1	2020	MS20-MAY: Cumulative Update F...	465292405	KB4556441	Patches for Windows	Security Update	05/12/2020
KB4558998	138453	CVE-2020-1346	High	High	1	2020	MS21-MAR: Servicing Stack Upd...	500089901	KB5000899	Patches for Windows	Security Update	03/09/2021
Security Up...	132999	CVE-2019-1206	High	High	2	2020	MS20-MAY: Cumulative Update F...	465292405	KB4556441	Patches for Windows	Security Update	05/12/2020

Figure 35. Detected Vulnerable Devices with Applicable Fixlets - Device Vulnerabilities

 **Vulnerability Device Summary** * BigFix Data

Vulnerability	Plugin 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 R...	468032515	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
3/6/2021	188793801-1	WIN-UTRHAU79H6U9	Win2019 10.0.17763.1071	172.17.128.1	Server	3/25/2021 4:57:12 PM
	548314002-5	WIN-8080L6N78	Win2010 6.0.6002.18045...	10.134.146.97	Laptop	3/25/2021 4:54:11 PM

Figure 36. Detected Vulnerable Devices with Applicable Fixlets - Device Detail

 **Device Detail Summary** * BigFix data

DeviceID	* Device Name	* IP Address	* OS	* Type	* Last Report Time
188793801-1	WIN-UTRHAU79H6U9	172.17.128.1	Win2019 10.0.17763.1071	Server	3/25/2021 4:57:12 PM

Vulnerability Detail

Vulnerability Title	Plugin ID	CVE List	CVSS2	Severity	Detected Date	* Fixlet Title	* Fixlet ID	* Fixlet Site	* Fixlet Sou.	* Fixlet Category	* Source Rel.
Adobe Flash Play...	137253	CVE-2020-3757	High	Medium	3/6/2021	MS20-OCT: Security Update for Adobe F...	468032515	Patches for Windows	KB4580325	Security Update	10/13/2020
KB4537759 Secur...	138618	CVE-2020-3757	High	Medium	3/6/2021	MS20-OCT: Security Update for Adobe F...	468032515	Patches for Windows	KB4580325	Security Update	10/13/2020
KB4518553 Wind...	138601	CVE-2019-1206	High	High	3/6/2021	MS20-MAY: Cumulative Update for .NET...	465292405	Patches for Windows	KB4556441	Security Update	05/12/2020
KB4558998 Wind...	138453	CVE-2020-1346	High	High	3/6/2021	MS21-MAR: Servicing Stack Update for...	500089901	Patches for Windows	KB5000899	Security Update	03/09/2021
Security Update...	132999	CVE-2019-1206	High	High	3/6/2021	MS20-MAY: Cumulative Update for .NET...	465292405	Patches for Windows	KB4556441	Security Update	05/12/2020
Security Update...	138600	CVE-2019-1206	Medium	Medium	3/6/2021	MS20-MAY: Cumulative Update for .NET...	465292405	Patches for Windows	KB4556441	Security Update	05/12/2020
Security Update...	138454	CVE-2020-1246	Medium	High	3/6/2021	MS20-OCT: Cumulative Update for .NET...	467896603	Patches for Windows	KB4579876	Security Update	10/13/2020
Security Update...	128742	CVE-2019-1206	Low	Low	3/6/2021	MS20-MAY: Cumulative Update for .NET...	465292405	Patches for Windows	KB4556441	Security Update	05/12/2020
Windows Specifi...	138251	CVE-2017-0715	Medium	High	3/6/2021	4072698: Enable mitigations to help pr...	407269805	Patches for Windows	KB4072698	Security Advis...	01/04/2018

Vulnerabilities without Available Fixlets

Figure 37. Detected Vulnerable Devices without Applicable Fixlets - Overview

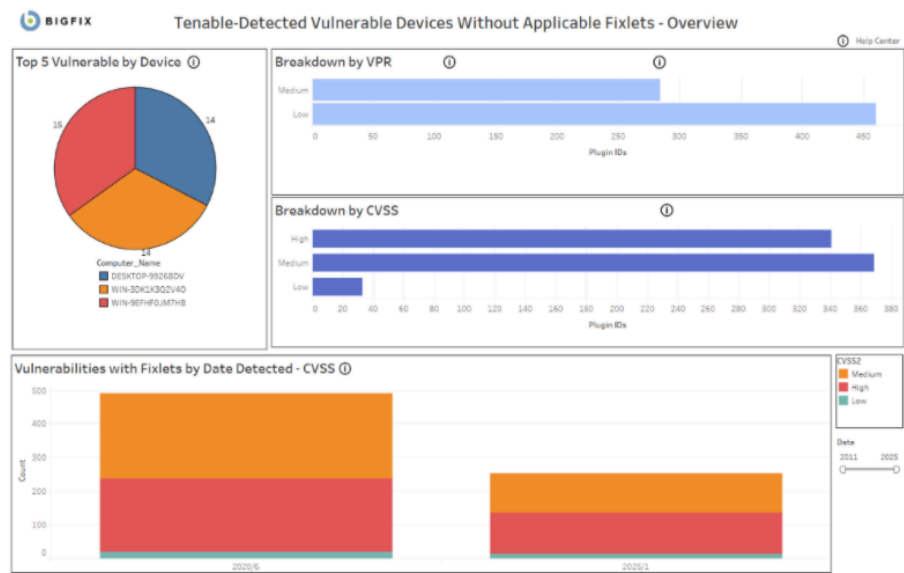


Figure 38. Detected Vulnerable Devices without Applicable Fixlets - Overview

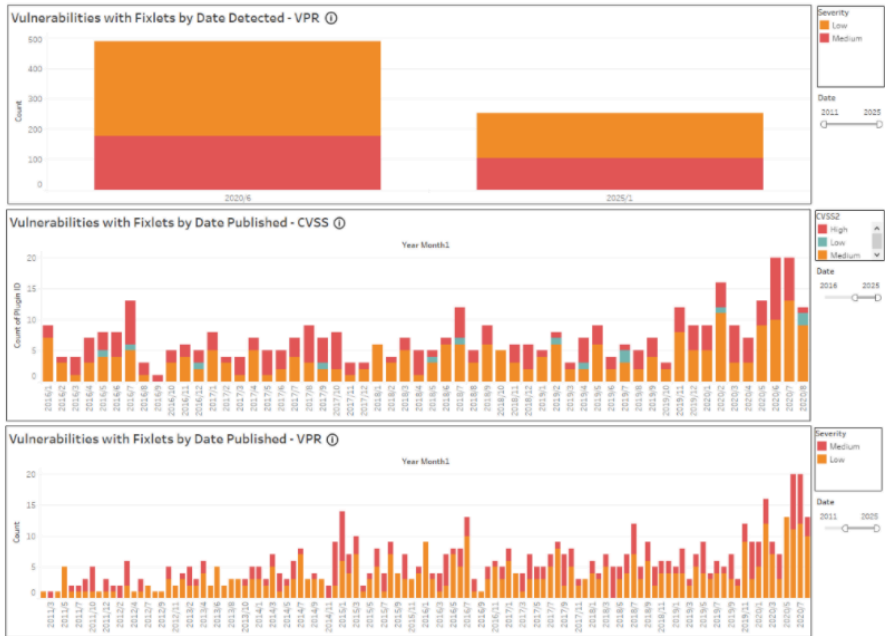


Figure 39. Detected Vulnerable Devices without Applicable Fixlets - Vulnerability List

BIGFIX

Right-click on Plugin ID to drill down

Vulnerability List

* BigFix data

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
Adrianus Fishere and Crucible Cross Site Scripting Vulnerability (CRUC-8381,FE-7163,CRUC-8380,FE-7164)	130422	Low	Low	1	2019
CentOS Security Update for libvirt (CESA-2012-1202)	120574	Low	Low	1	2012
CentOS Security Update for libvirt (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)	117516	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-2015-13405)	124023	Low	Low	1	2015
Fedora Security Update for qemu (FEDORA-2016-1a354bfa4)	276023	Low	Low	1	2016
Fedora Security Update for slapi-nis (FEDORA-2014-1442)	122951	Low	Low	1	2015
Fedora Security Update for suse (FEDORA-2015-2247)	123347	Low	Low	1	2015
Fedora Security Update for xen (FEDORA-2016-daf6b1d277b)	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 libvm (openSUSE-SU-2015-0246-1)	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 libcrypt (ELSA-2013-1407)	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	10643	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-2014-0946-1)	167211	Low	Low	1	2014
SUSE Enterprise Linux Security Update for libcap1 (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 libbth (openSUSE-SU-2013-0404-1)	166870	Low	Low	1	2013

Figure 40. Detected Vulnerable Devices without Applicable Fixlets - Device Vulnerabilities

BIGFIX 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-9EFHFQJMT7HB	Win2016 10.0.14393.1884	10.134.146.136	Server	2/16/2021 4:11:07 PM	351628

Figure 41. Detected Vulnerable Devices without Applicable Fixlets - Device Detail

BIGFIX Device Detail Summary * BigFix data

* Device Name	DeviceID	* IP Address	* OS	* Type	* Last Report Time
WIN-9EFHFQJMT7HB	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)	370284	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 gcc 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 (JIRASERVER-69784, JIRASERVER-69783, JIRASERVER-69782, JIRASERVER-69781, JIRASERVER-69780)	13609	Medium	Low	6/16/2020
Atlassian Jira Server and Data Center Improper Authorization Vulnerability (JIRASERVER-70526)	13831	Medium	Low	6/16/2020
CentOS Security Update for Firefox (CESA-2012-1210)	120570	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-2019-2693)	256402	High	Medium	1/1/2025
CentOS Security Update for Rtmpack (CESA-2019-0375)	256673	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 Discrepancies

Figure 42. Vulnerability Discrepancies - Overview

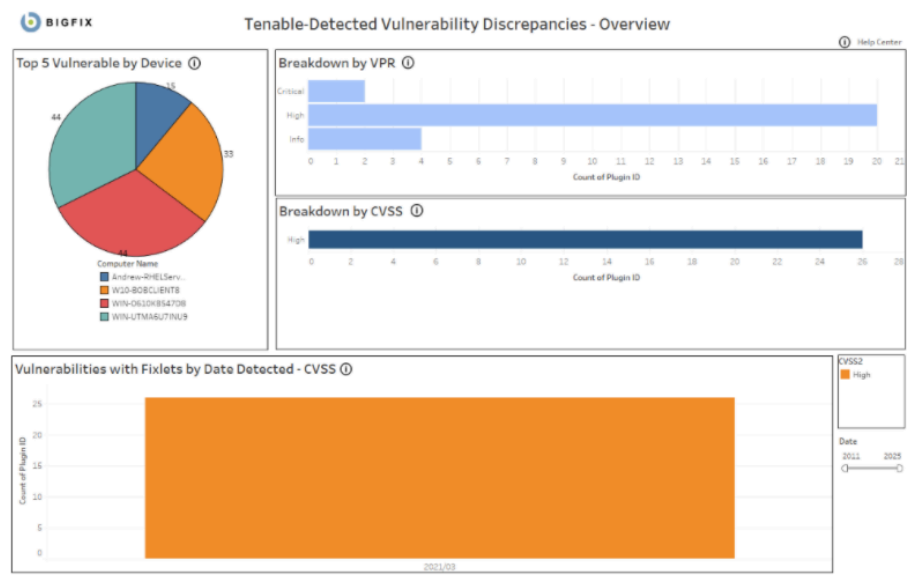


Figure 43. Vulnerability Discrepancies - Overview

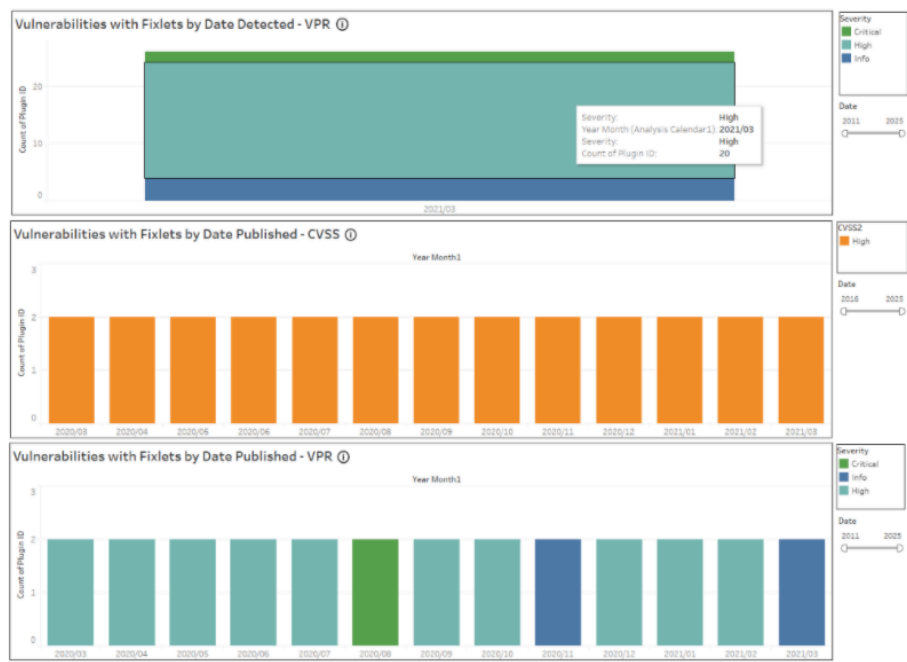


Figure 44. Vulnerability Discrepancies - Vulnerability List

 **Tenable-Detected Vulnerability Discrepancies - Detail** * Bigfix date

Right-click on Plugin ID to drill down

Vulnerability	Plugin ID	CVE_List	CVSS2	Severity	Applicable...	Year of Pub.	* Fictet Title	* Fictet ID	* Fictet Sou.	* Fictet Site	* Fictet Category	* Source Rel.
KB4586793	142693	CVE-2020-0...	High	Info	1	2020	MS21-MAR: Cumulative Update for Windo...	S00082201	KB5000822	Patches for Windows	Security Update	03/09/2021
KB4586830	142690	CVE-2020-0...	High	Info	1	2020	MS21-MAR: Cumulative Update for Windo...	S00082201	KB5000822	Patches for Windows	Security Update	03/09/2021
KB5000803	147222	CVE-2020-0...	High	Info	1	2021	MS21-MAR: Cumulative Update for Windo...	S00082201	KB5000822	Patches for Windows	Security Update	03/09/2021
KB5000822	147223	CVE-2020-0...	High	Info	1	2021	MS21-MAR: Cumulative Update for Windo...	S00082201	KB5000822	Patches for Windows	Security Update	03/09/2021

Figure 45. Vulnerability Discrepancies - Device Vulnerabilities

 **Tenable-Detected Vulnerability Discrepancies - Device Summary** * Bigfix Date

Vulnerability	Plugin ID	CVE_List	Year of Pub.	CVSS2	Severity	* Fictet Title	* Fictet ID	* Fictet Site	* Fictet Sou.	* Fictet Category	* Source Rel.
KB4586793	142693	CVE-2020-0645, CVE-2...	2020	High	Info	MS21-MAR: Cumulative Update for Windows...	S00082201	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-UTMA6U71NU9	Win2019 10.0.17763.107 (1809)	172.17.128.1	Server	3/25/2021 4:57:12 PM

Figure 46. Vulnerability Discrepancies - Device Detail

 **Tenable-Detected Vulnerability Discrepancies - Device Summary** * Bigfix date

DeviceID	* Device Name	* IP Address	* OS	* Type	* Last Report Time
10373101-1	WIN-UTMA6U71NU9	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	* Fictet Title	* Fictet ID	* Fictet Site	* Fictet Sou.	* Fictet Category	* Source Rel.
KB4538461: Wind...	134368	CVE-2020-0645, CVE-2...	High	High	3/8/2021	MS21-MAR: Cumulative Update for...	S00082201	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...	S00082201	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...	S00082201	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...	S00082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4561608: Wind...	137196	CVE-2020-0645, CVE-2...	High	High	3/8/2021	MS21-MAR: Cumulative Update for...	S00082201	Patches for Windows	KB5000822	Security Update	03/09/2021
KB4565349: Wind...	139488	CVE-2020-0645, CVE-2...	High	Critical	3/8/2021	MS21-MAR: Cumulative Update for...	S00082201	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...	S00082201	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...	S00082201	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...	S00082201	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...	S00082201	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...	S00082201	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...	S00082201	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...	S00082201	Patches for Windows	KB5000822	Security Update	03/09/2021

Chapter 6. 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. 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 2. Attribute details of the configuration file.

Attribute name	Default value	Required	Description
datasource-name	N/A	Yes	This attribute is used to uniquely identify the data-source. With this attribute, data-sources can be mapped to specific adapters

Table 2. Attribute details of the configuration file. (continued)

Attribute name	Default value	Required	Description
			within each data flow.
connectionstring	N/A	Yes	URL of the respective data sources. For example: <code>https://[Qualys-APIURL],https://[TenableAPI-URL]:443</code>
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

Table 2. Attribute details of the configuration file. (continued)

Attribute name	Default value	Required	Description
			being persisted in the configuration file.
verifycert	True	No	This attribute enables or disables SSL certificate validation with this data source.

<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 3. Attribute details of the configuration file.

Attribute name	Required	Description
displayname	Yes	This attribute is used to describe the individual data flow.
datatype	Yes	Type: Int
executionintervalinminutes	Yes	

<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 4. 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 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 5. Attribute details of the configuration file.

Attribute name	Required	Description
displayname	Yes	This attribute is used to describe this adapter configuration.
adapterclass	Yes	insight 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.

```
<dataflow displayname="Endpoint data from Qualys To Bigfix Insights" datatype="finding" executionintervalinminute:
  <dataflowdescription/>
  <sourceadapter displayname="Qualys Adapter" adapterclass="qualys" datasourcenname="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" datasourcenname="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>
```

<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 6. Attribute details of the configuration file.

Attribute name	Required	Description
displayname	Yes	This attribute is used to describe the property being configured.
columnname	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 confi-

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

Attribute name	Required	Description
		dence 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 \(on page 41\)](#).

Table 7. 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
LogLevel	String	DEBUG	Sets the logging level for the service.	• INFO • DEBUG • ERROR

Setting name	Data type	Default value	Description	Possible values
lvr_in-sight.worker_threads	Int	8	Sets the number of worker process (for Corellation) that can be run concurrently.	
Logger.RetentionInDays	Int	5	Indicates the duration of log that you want to retain.	
NumberOf-Concurrent-Dataflows	Int	1	Sets the number of dataflow processors that can be run concurrently.	
Data-Flow.QueueRefreshInterval	Int	120	The time interval at which the data flow is refreshed.	
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 name	Data type	Default value	Description	Possible values
			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 <code>qualys.batch_size</code> 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).	
PurgeFindingsOnExecutionOfDataflow		FALSE		When set to true, will attempt to purge all *invalid ivr data associat-

Setting name	Data type	Default value	Description	Possible values
				ed with the current dataflow configuration (from which we generate a hash), as well as all data <i>*not*</i> associated with existing dataflow configurations. <i>*invalid</i> - 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

Setting name	Data type	Default value	Description	Possible values
				 is performed (regardless of this setting) to attempt to automatically remove all invalid data (again, that is, data in IVR tables linked to a hash that was calculated from a dataflow configuration that

Setting name	Data type	Default value	Description	Possible values
				 has been changed/modified by the user).

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.

```

.\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 service.
  --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 8. List of command line arguments.

Command	Purpose	Additional information
--ProvideCredentials <Data-SourceName>	To securely capture credentials for single datasource	
--provideCredentials	To securely capture credentials for all data-sources	
--ValidateConfiguration	To validate the configuration	
--InitializeSchemas	To initialize the schema	



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 everyday. 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

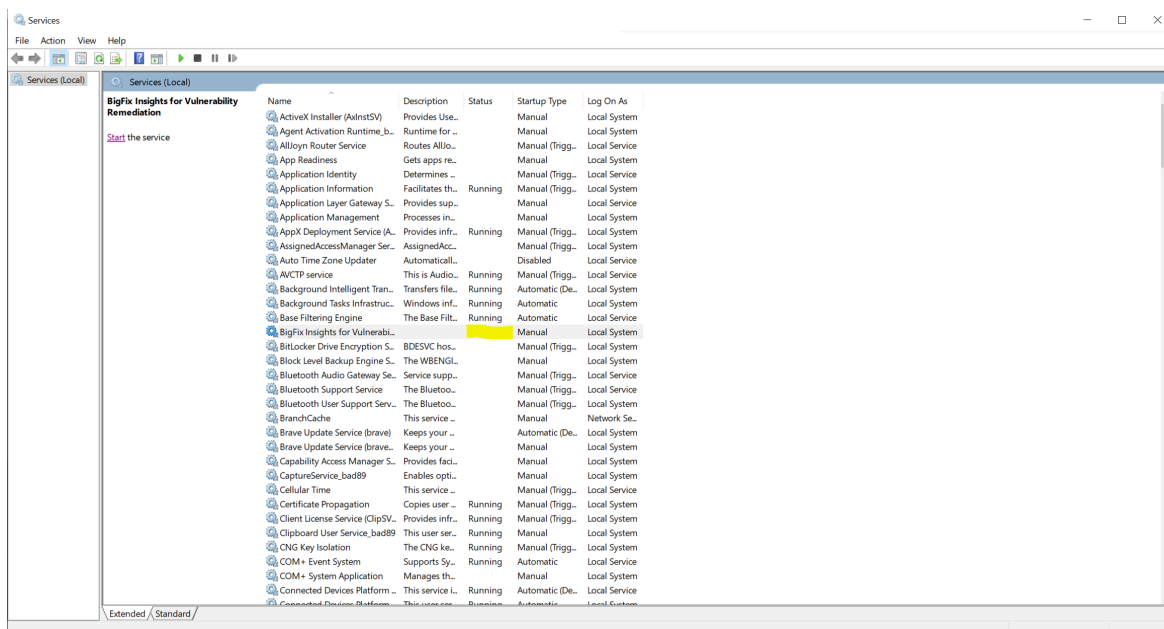
With DEBUG enabled, this log file contains detailed logging information related to the primary processes. It should show issues related to service start and configuration.

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.



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

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

```

29 2021-03-20 23:13:27.730910 3896 DataFlowRunner LogLevels.DEBUG Executing DataFlow Task : Endpoint data from Qualys To Bigfix Insights
30 2021-03-20 23:13:27.730910 3896 GetDataSource LogLevels.DEBUG Read Single Datasource details: QualysAPI
31 2021-03-20 23:13:27.730910 3896 GetDataSource LogLevels.DEBUG Read Single Datasource details: BigfixINSIGHT
32 2021-03-20 23:13:27.746534 3896 __init__ LogLevels.DEBUG DataFlow Initialized
33 2021-03-20 23:13:27.746534 3896 execute LogLevels.INFO Starting DataFlow: Endpoint data from Qualys To Bigfix Insights
34 2021-03-20 23:13:27.746534 3896 validate_configuration LogLevels.DEBUG Validating Configuration
35 2021-03-20 23:13:27.746534 3896 validate_configuration LogLevels.DEBUG Source Adapter Validation: qualys
36 2021-03-20 23:13:27.762156 3896 ExecuteRESTCommand LogLevels.INFO Executing REST Command

```

Table 9. 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.

Known limitations

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

1. IVR Tenable.sc:



Warning: Sessions are not terminated as expected. Over a period of time, tenable does not allow to proceed as the maximum limits allowed is 10 user per session.

2. IVR(BigFix Insights for Vulnerability Remediation)1.0 currently officially supports BigFix Insights instances with only one BigFix Datasource.

3. IVR Tenable.sc: Allow Session Management must be disabled. For more information, refer to the [Tenable.sc configuration settings](#).



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



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

6. Currently we do not support multi-instance data flow service even for the same datasource type.

7. PowerBI and Tableau reports: The maximum number of records which can be exported to CSV file:

- 50k records for Tableau
- 30k records for PowerBI

8. 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.

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 nonpreferred 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 \(on page 51\)](#) [B \(on page 52\)](#) [C \(on page 52\)](#) [D \(on page 54\)](#) [E \(on page 57\)](#) [F \(on page 57\)](#) [G \(on page 57\)](#) [L \(on page 57\)](#) [M \(on page 58\)](#) [N \(on page 59\)](#) [O \(on page 59\)](#) [P \(on page 59\)](#) [R \(on page 60\)](#) [S \(on page 60\)](#) [T \(on page 63\)](#) [U \(on page 63\)](#) [V \(on page 63\)](#) [W \(on page 63\)](#)

A

action

1. See [Fixlet \(on page 57\)](#).
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 \(on page 52\)](#).

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 \(on page 53\)](#).

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 \(on page 55\)](#).

BigFix agent

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

BigFix client

See [BigFix agent \(on page 52\)](#).

BigFix console

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

C

client

A software program or computer that requests services from a server. See also [server \(on page 61\)](#).

client time

The local time on a BigFix client's 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 \(on page 59\)](#).

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 \(on page 55\)](#).

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 \(on page 52\)](#) and [manual computer group \(on page 58\)](#).

console

See [BigFix console \(on page 52\)](#).

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 \(on page 56\)](#).

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 \(on page 53\)](#).

CVE ID

See [Common Vulnerabilities and Exposures Identification Number \(on page 53\)](#).

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 \(on page 52\)](#), [component \(on page 53\)](#), [deployment window \(on page 55\)](#), and [multiple action group \(on page 58\)](#).

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 \(on page 55\)](#).

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 \(on page 54\)](#).

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 \(on page 56\)](#).

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.

G

group deployment

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

H

Hybrid cloud

The utilization of distinct sets of cloud services (typically public and private) with integration and/or orchestration across them.

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 \(on page 58\)](#).

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 \(on page 53\)](#).

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.

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 \(on page 55\)](#).

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 \(on page 53\)](#).

NVD

See [National Vulnerability Database \(on page 59\)](#).

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 \(on page 61\)](#).

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 \(on page 52\)](#).

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 \(on page 54\)](#).

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 \(on page 63\)](#).

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 \(on page 64\)](#).

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.