BigFix

Known Exploited Vulnerabilities Content Pack Add-on User Guide

Special notice

Before using this information and the product it supports, read the information in Notices *(on page x)*.

Edition notice

This edition applies to BigFix version 11 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. CISA Known Exploited Vulnerabilities: Overview

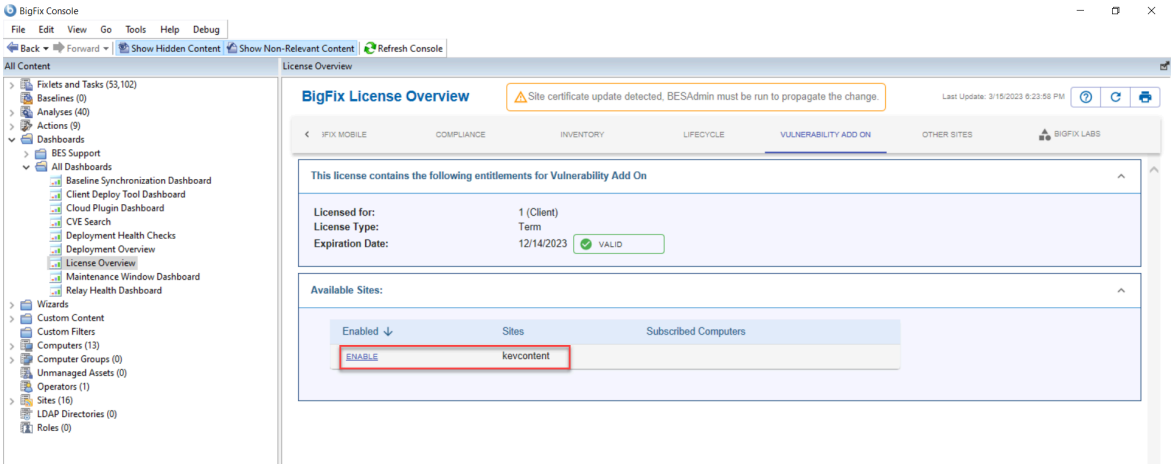
The Known Exploited Vulnerabilities (KEV) Content Pack is available as an **add-on** for BigFix. It is a collection of BigFix Fixlets that is derived from extensive research of the CISA KEV catalog, NVD, and Vendor Advisories. This KEV Content Pack provides BigFix operators with the ability to quickly identify endpoints with vulnerabilities that are high-risk and time-sensitive given that they are known to have been exploited or are actively being exploited.

The KEV Content Pack focuses on vulnerabilities associated with the devices that are in-scope for BigFix. For a list of supported CVEs, refer to BigFix Wiki at BigFix Known Exploited Vulnerabilities (KEV) Content Pack.

Chapter 2. Enable BigFix KEV Content Pack Site

This topic provides instructions on how to enable the Known Exploited Vulnerabilities (KEV) Content Pack and subscribe computers to the site.

1. In the License Overview Dashboard navigate to the **Vulnerability Add On** domain.
2. In the site list, find the **kevcontent** site and click **Enable**. The site gets enabled.

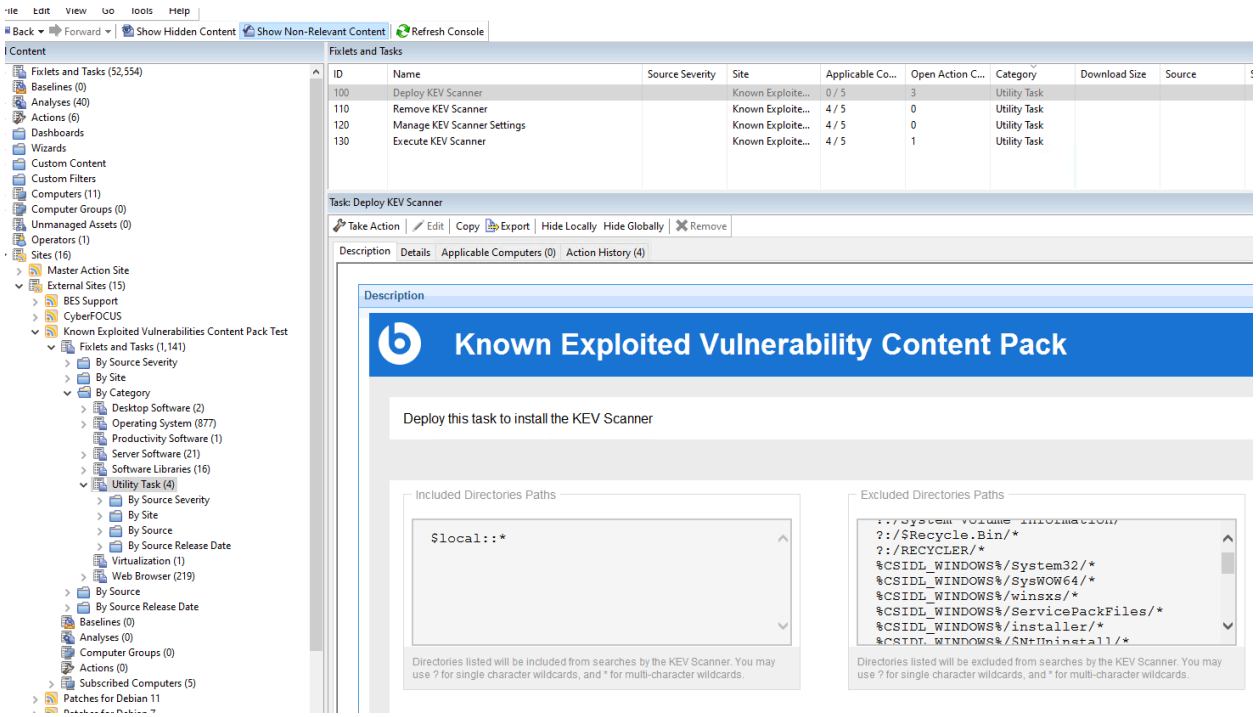


3. To subscribe computers to the site, click the site name.
4. From the **Computer Subscriptions** tab, indicate which subset of your BigFix Client computers you want to subscribe to this site. Select a suitable option:
    - **All Computers**. Select this option to automatically subscribe all Clients to this site.
    - **No Computers**. Select this option if you are not yet ready to subscribe any computers.
    - **Computers which match the condition below**. Select this option to describe a set of criteria that must all evaluate to TRUE before a BigFix Client is subscribed. From the pull-down menu, you can select from dozens of properties to test for inclusion.

    For information on how to subscribe computers to the site, refer to Computer Subscriptions Tab.

Chapter 3. KEV Scanner Policy Action Management

BigFix provides four utility tasks to facilitate the deployment, execution, and configuration of the Known Exploited Vulnerabilities (KEV) Scanner. The KEV Scanner is necessary to identify certain CVEs (for more details on which CVEs require the KEV Scanner, refer to BigFix Wiki at BigFix Known Exploited Vulnerabilities (KEV) Content Pack).



- **Task 100**: Deploy KEV Scanner. This task is used to produce a policy action to deploy the KEV Scanner on endpoints in your environment.
- **Task 110**: Remove KEV Scanner. This task is used to remove the KEV Scanner and any artifacts on an endpoint.
- **Task 120**: Manage KEV Scanner Settings. This task is used to manage settings on an endpoint, where the KEV Scanner is deployed.
- **Task 130**: Execute KEV Scanner. This task is used to periodically execute the KEV Scanner on the endpoint.

Note: You can prevent the KEV Scanner from being executed on any device by applying the `KEV_Deny` client setting with the value as 1 on that device. For more information on client settings and how to apply them, refer to List of settings and detailed descriptions.

- **Included Directory Paths/Excluded Directory Paths**

  These are path wildcards that can be leveraged to direct the scanner on where or where not to search. These wildcard paths may leverage environment variables, ? for signal character matching, and * for zero or more character matching.

- **CPU Throttling Threshold**
  - This setting limits the CPU Utilization of the scanner on the endpoint to roughly a certain percentage of the CPU.
  - Default: 100

Chapter 4. CVE probe management

This topic provides instructions on how to enable the CVE Detection Probes for the target operating systems.

To minimize the impact of this content pack to the evaluation loop of our BigFix agent, a Probe Task has been developed for each type of operating system (Windows, Linux and MacOS) to enable the consolidation and scheduling of resource intensive vulnerability detection methodologies. You can deploy these probe tasks as policy actions, with a recommended interval of once per day.

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.