BigFix 10 Technology Preview: Compliance Vulnerability Reporting

HCL SOFTWARE

BigFix 10 Technology Preview

Purpose

- To evaluate customer experience and solicit feedback on the major features of BigFix v10 and to identify possible enhancement areas

When

- January 27 – February 21

Approach

- Your Technology Preview contact will provide you with:
  - Hosted environment and access credentials
  - Program Guide gives you an overview of all the BigFix 10 Technology Preview available
  - This video gives you an overview of the Compliance Vulnerability Reporting Technology Preview program
  - Compliance Vulnerability Reporting Overview is the presentation the video is going through
  - Feedback link to capture and submit feedback

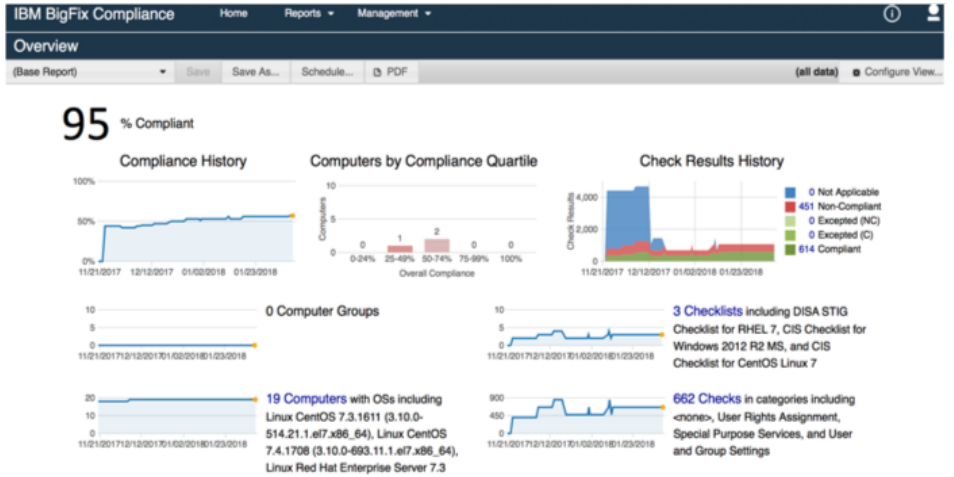
Background

HCL SOFTWARE

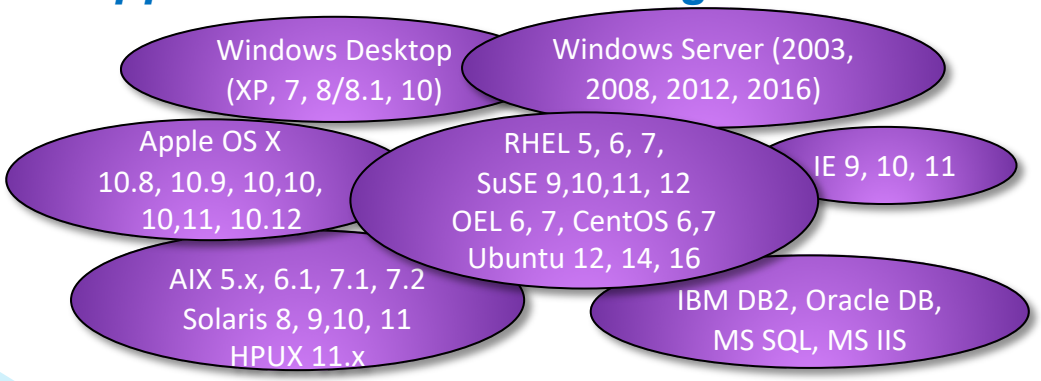
BigFix Compliance – Ensuring Continuous Regulatory / Policy Compliance

- ***Real-time visibility and continuous monitoring and remediation to reduce security risk***

- ***Analytics and reporting of current status and historical trend for accurate posture assessment***



- ***Support over 60 Operating Systems, Middleware & Applications to meet all organization needs***



- ***20,000+ 'out of the box' checks to support benchmarks from CIS, DISA, USGCB, PCI DSS***

CIS Center for Internet Security® DISA PCI DSS COMPLIANT NIST SCAP

Evolving BigFix Compliance to Patch / Vulnerability Reporting

Customer Challenges

- Patch / Vulnerability posture not so visible

No data to give a comprehensive and accumulative view of the patching actions and how the vulnerabilities have been remediated over time

- Not effective vulnerability remediation

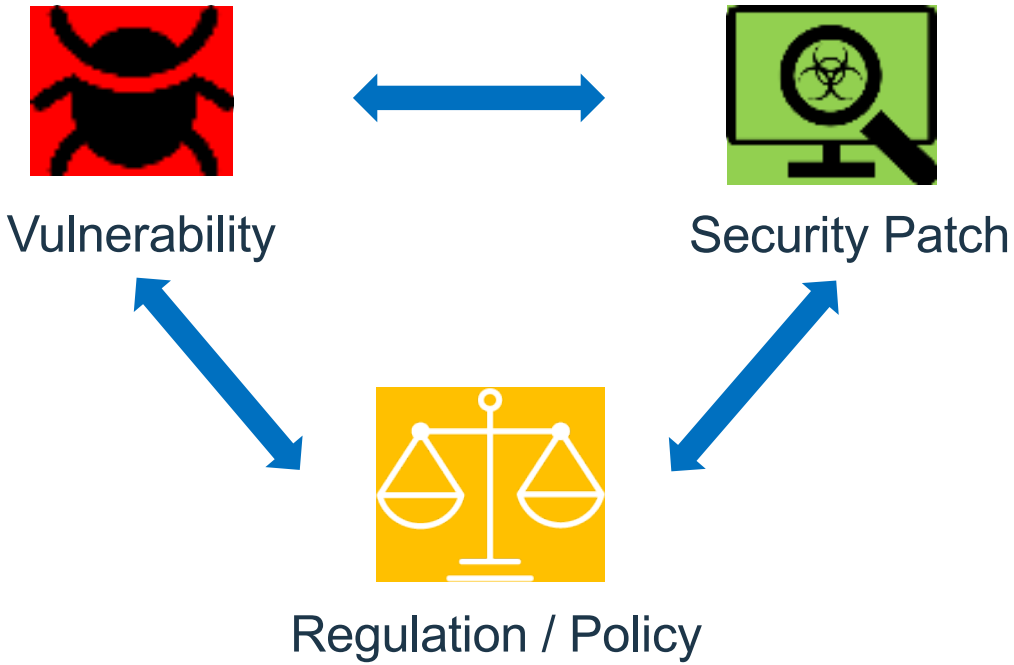
Not enough information to help IT Ops prioritize their patching efforts to maximize the impact to the security posture and increase their productivity

- Difficulty in demonstrating compliance

Incapable to demonstrate in auditing how and when security patches were applied or critical or high severity vulnerabilities were remediated

Solution: Patch / Vulnerability Reporting

To extend BigFix Compliance's capabilities to track endpoint patching and vulnerability posture and historical trend, show the relationship between patching activity and vulnerability status change, and help prioritize remediation actions.



BigFix Compliance – Vulnerability Reporting

Extension of Patching Reporting (delivered in 4Q 2018) to focus on tracking and reporting of endpoints' vulnerability posture as result of patching actions, to enable customers to identify risks and demonstrate compliance in a broader manner

➢ Risk Posture Assessment

→ A **SOC Manager** or **Security Analyst** can get the current status, historical trend and details of vulnerabilities of various severities existed on each endpoint or across the environment.

➢ Remediation Task Prioritization

→ An **IT Operations Specialist** can get more information to help him more effectively prioritize his patching actions to maximize the impact to the vulnerability posture change.

➢ Vulnerability Compliance Reporting

→ A **Compliance Specialist** can report how vulnerabilities have been remediated by patching actions to demonstrate compliance with specific regulatory or organization policies.

Compliance Vulnerability Reporting

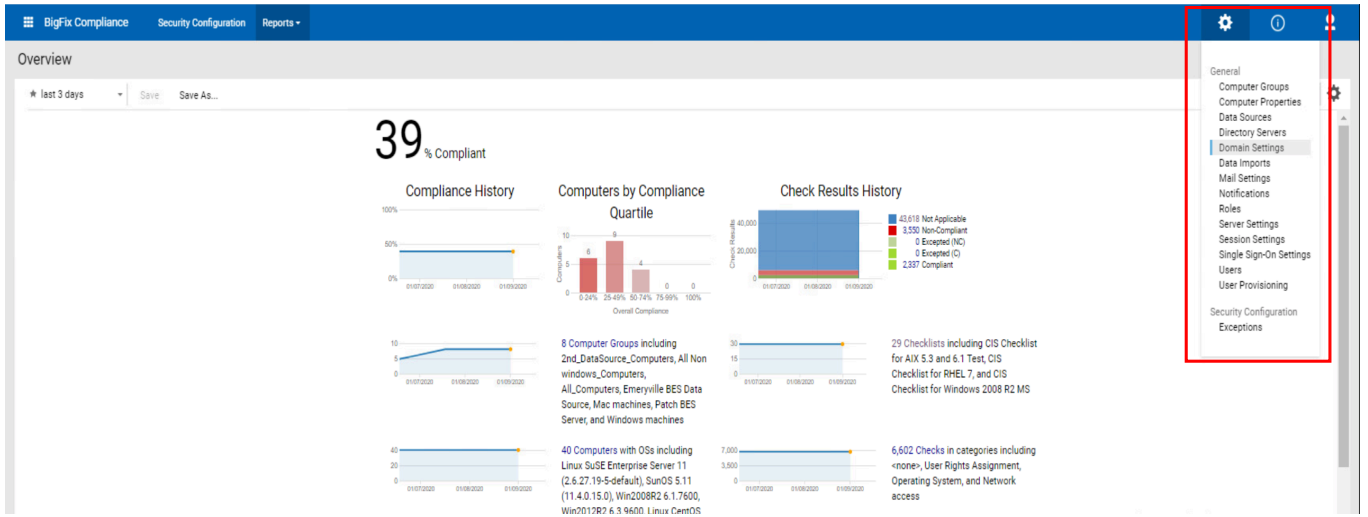
HCL SOFTWARE

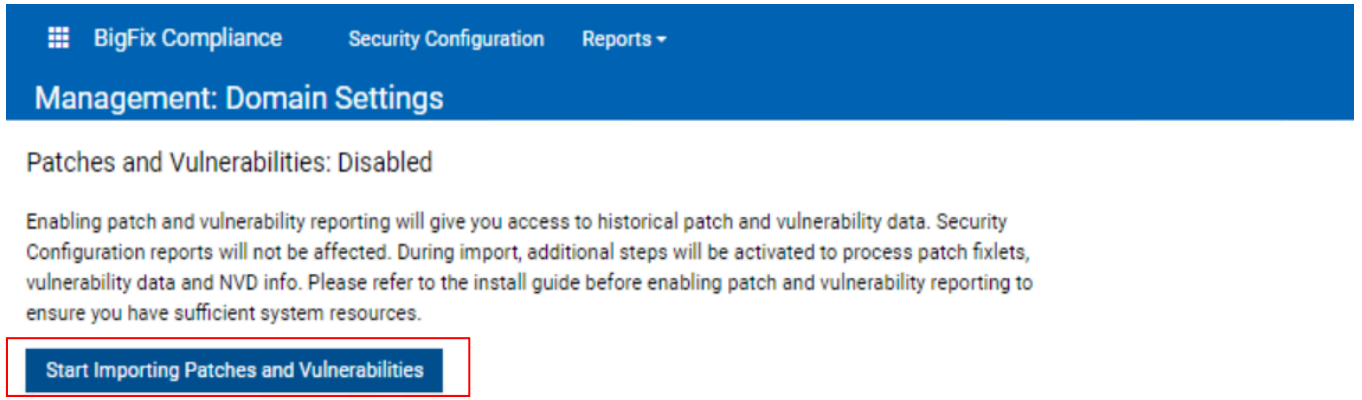
A Summary of the Vulnerability Reporting feature

- Enablement of Vulnerability Reporting
- Domain and Report Navigation
- Vulnerability Posture Overview
- Vulnerability List
- Vulnerability Overview and Sub-reports
- Computer List
- Computer Overview and Sub-reports
- Computer Group List
- Computer Group Overview and Sub-reports

Enablement of Vulnerability Reporting

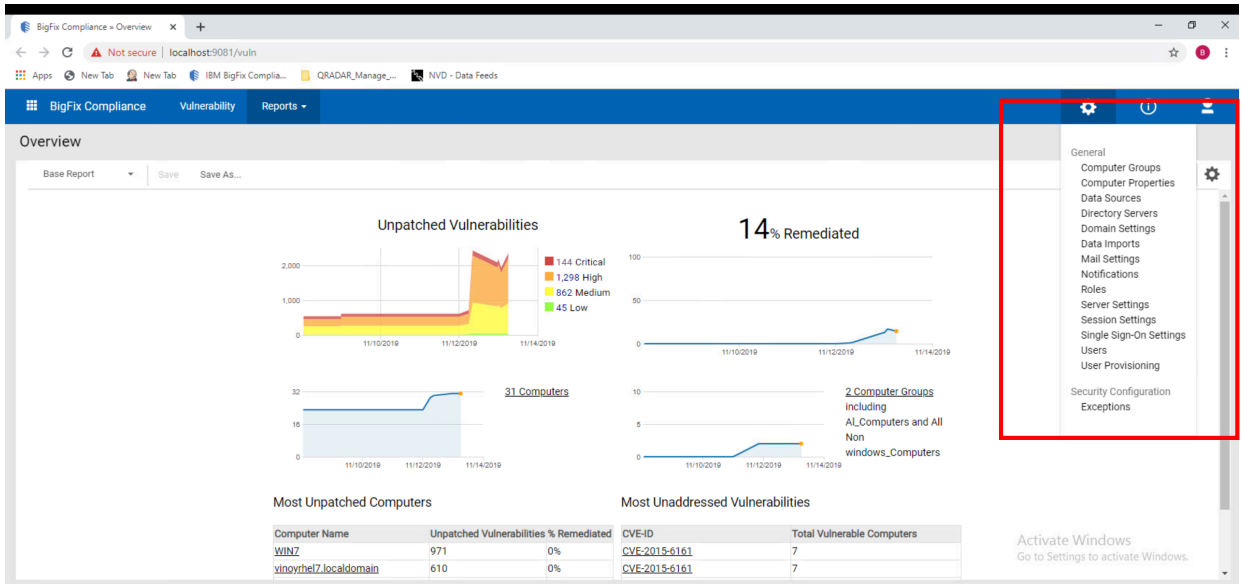
- All management configurations are accessible via a ‘gear’ at the top of the menu bar.
- Patch and Vulnerability Reporting need to be enabled first.
- Then, patch and vulnerability data need to be imported to SCA.

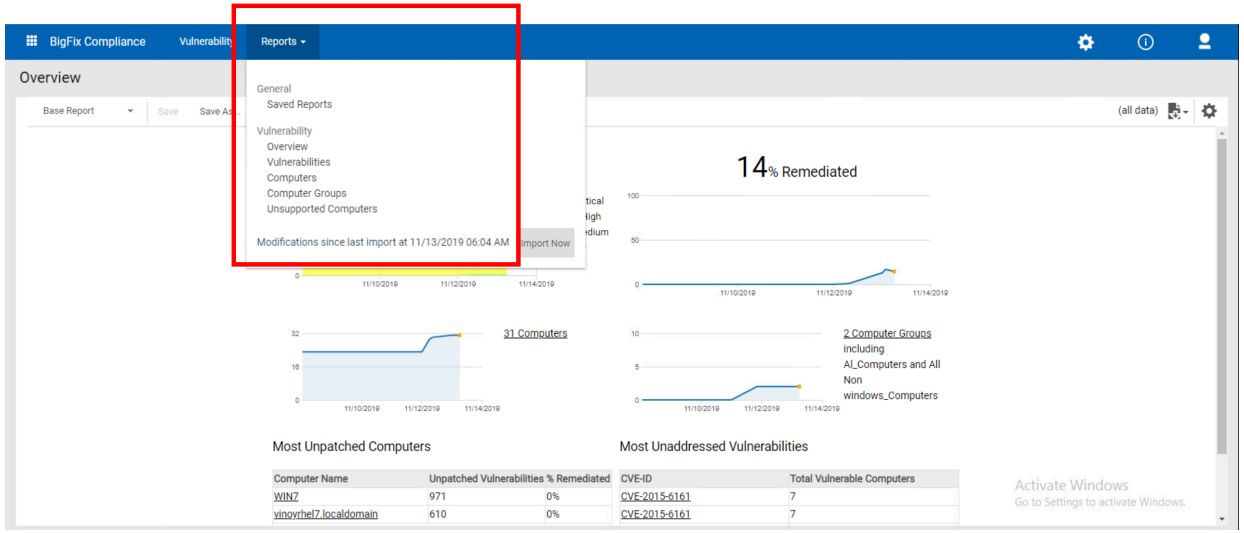




Domain and Report Navigation

- Three domains in SCA: Security Configuration, Patch, and Vulnerability
- Switching easily from one domain to another. Each domain has its own drop-down report menu.
- All management configurations accessible via a ‘gear’ at the top of the menu bar.
- All sub-reports now displayed as tabs, instead of using a drop-down menu before.
- Each report configurable via a smaller ‘gear’ at the top right of the report.
- A linkage between a Patch report and a Vulnerability report, whenever appropriate

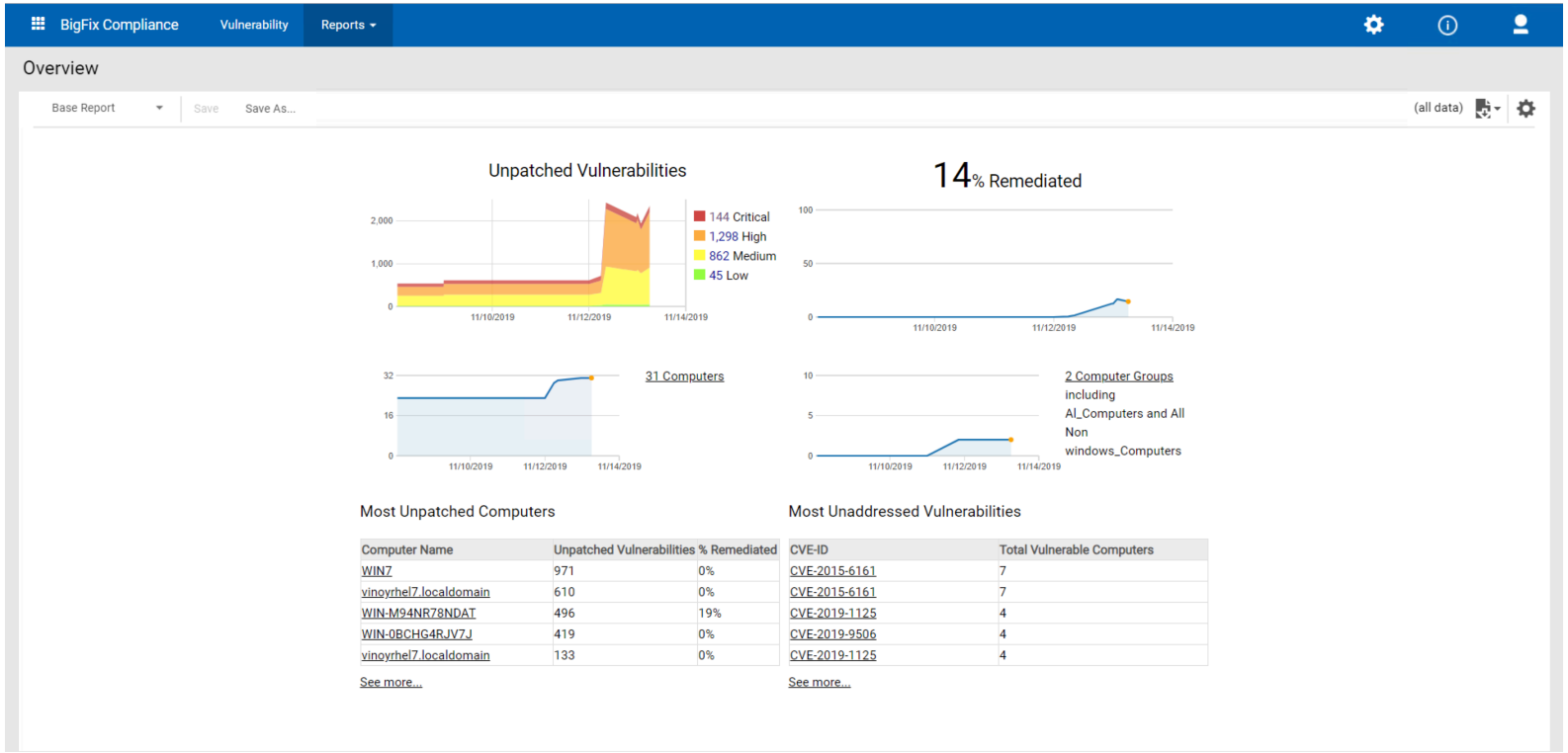




HCL SOFTWARE

Vulnerability Posture Overview

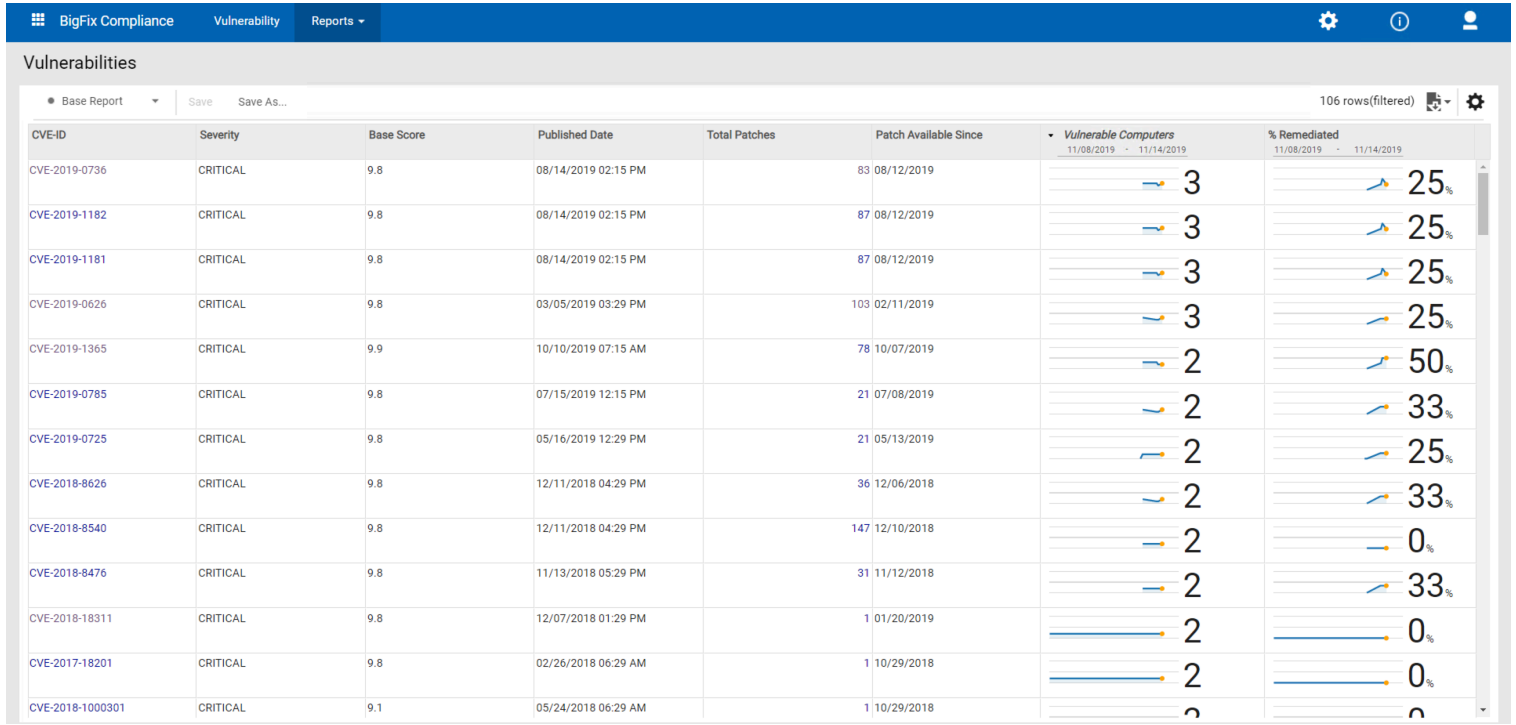
- A trending of the total number of unpatched vulnerabilities in each severity
- A trending of the percentage of remediated (patched) vulnerabilities
- A trending of all the computers and computer groups in the environment
- The computers that have the greatest number of unpatched vulnerabilities
- The vulnerabilities that have not been addressed with the greatest number of computers



HCL SOFTWARE

Vulnerability List

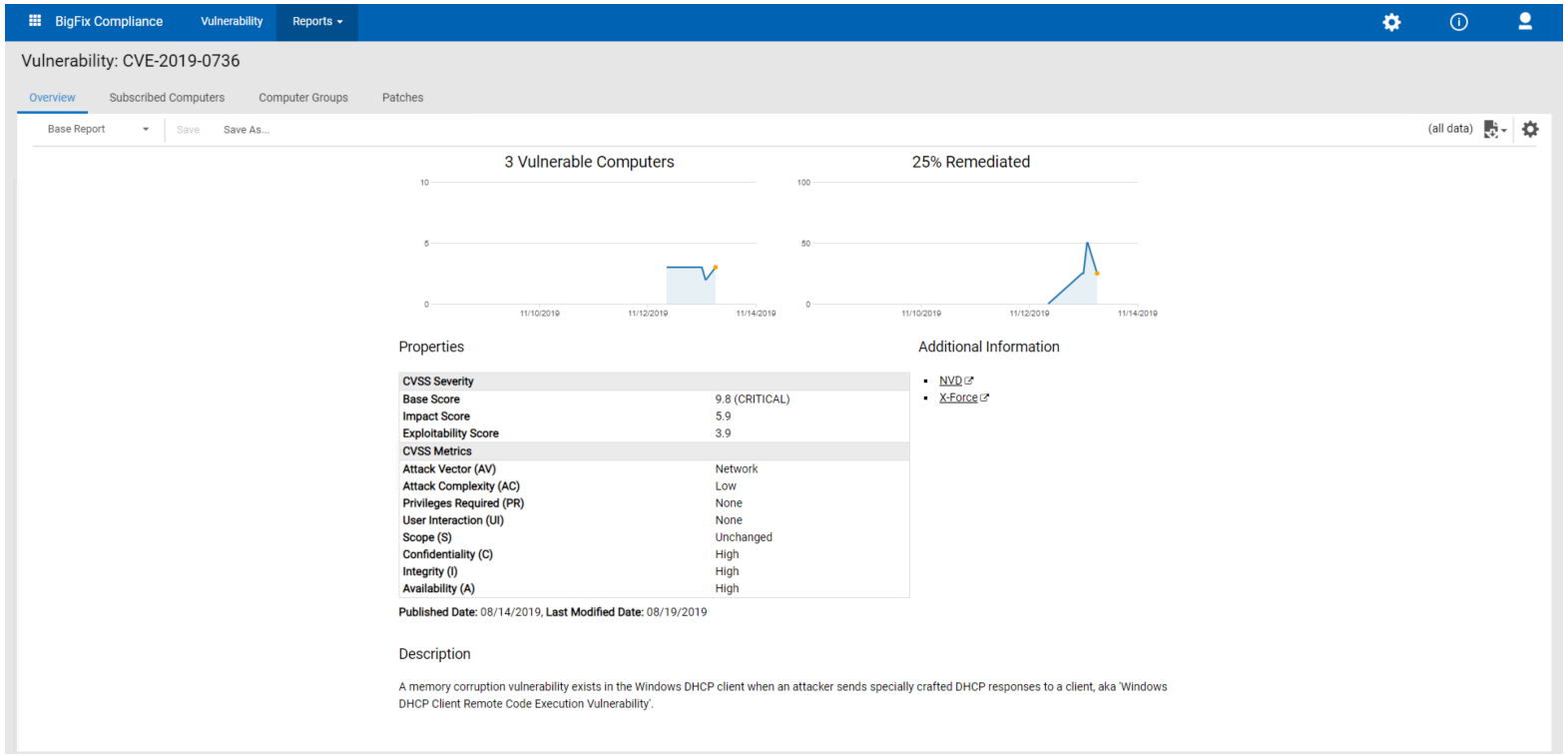
- All the CVEs being tracked, either remediated or not remediated
- Each CVE's basic properties, how many patches contain the fix. And when the first patch was available
- A trending and the current count of the computers that are still vulnerable
- A trending of the percentage of the computers that have been remediated
- Sorting data based on severity, vulnerable computers or remediation status to identify the vulnerabilities that need attention



CVE-ID	Severity	Base Score	Published Date	Total Patches	Patch Available Since	Vulnerable Computers 11/08/2019 - 11/14/2019	% Remediated 11/08/2019 - 11/14/2019
CVE-2019-0736	CRITICAL	9.8	08/14/2019 02:15 PM	83	08/12/2019	3	25%
CVE-2019-1182	CRITICAL	9.8	08/14/2019 02:15 PM	87	08/12/2019	3	25%
CVE-2019-1181	CRITICAL	9.8	08/14/2019 02:15 PM	87	08/12/2019	3	25%
CVE-2019-0626	CRITICAL	9.8	03/05/2019 03:29 PM	103	02/11/2019	3	25%
CVE-2019-1365	CRITICAL	9.9	10/10/2019 07:15 AM	78	10/07/2019	2	50%
CVE-2019-0785	CRITICAL	9.8	07/15/2019 12:15 PM	21	07/08/2019	2	33%
CVE-2019-0725	CRITICAL	9.8	05/16/2019 12:29 PM	21	05/13/2019	2	25%
CVE-2018-8626	CRITICAL	9.8	12/11/2018 04:29 PM	36	12/06/2018	2	33%
CVE-2018-8540	CRITICAL	9.8	12/11/2018 04:29 PM	147	12/10/2018	2	0%
CVE-2018-8476	CRITICAL	9.8	11/13/2018 05:29 PM	31	11/12/2018	2	33%
CVE-2018-18311	CRITICAL	9.8	12/07/2018 01:29 PM	1	01/20/2019	2	0%
CVE-2017-18201	CRITICAL	9.8	02/26/2018 06:29 AM	1	10/29/2018	2	0%
CVE-2018-1000301	CRITICAL	9.1	05/24/2018 06:29 AM	1	10/29/2018		

Vulnerability Overview

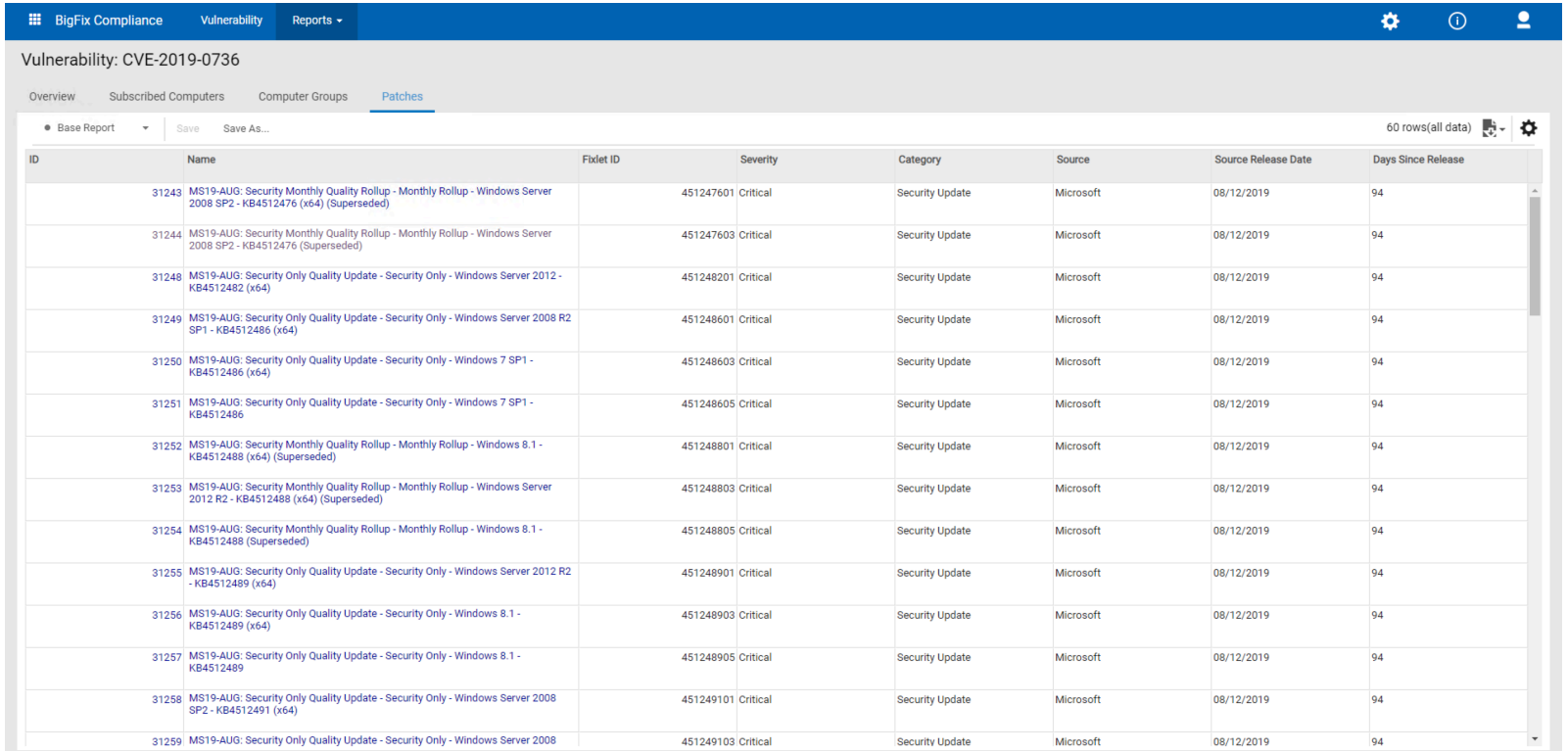
- A trending of the number of the computers that are still vulnerable
- A trending of the percentage of remediated computers
- The CVE properties and links to NVD and IBM X-Force for more information



HCL SOFTWARE

Vulnerability – Patch Sub-report

- All the patches that are available to address the vulnerability
- Each patch's properties including Fixlet ID, severity, source, release date, # of applicable computers, supersedence, etc.
- Clicking on the patch link to go to the patch report (in the Patch domain) to see more details
- Sorting all patches based on various properties (e.g., based on # of applicable computers) to determine what patches should be prioritized to apply

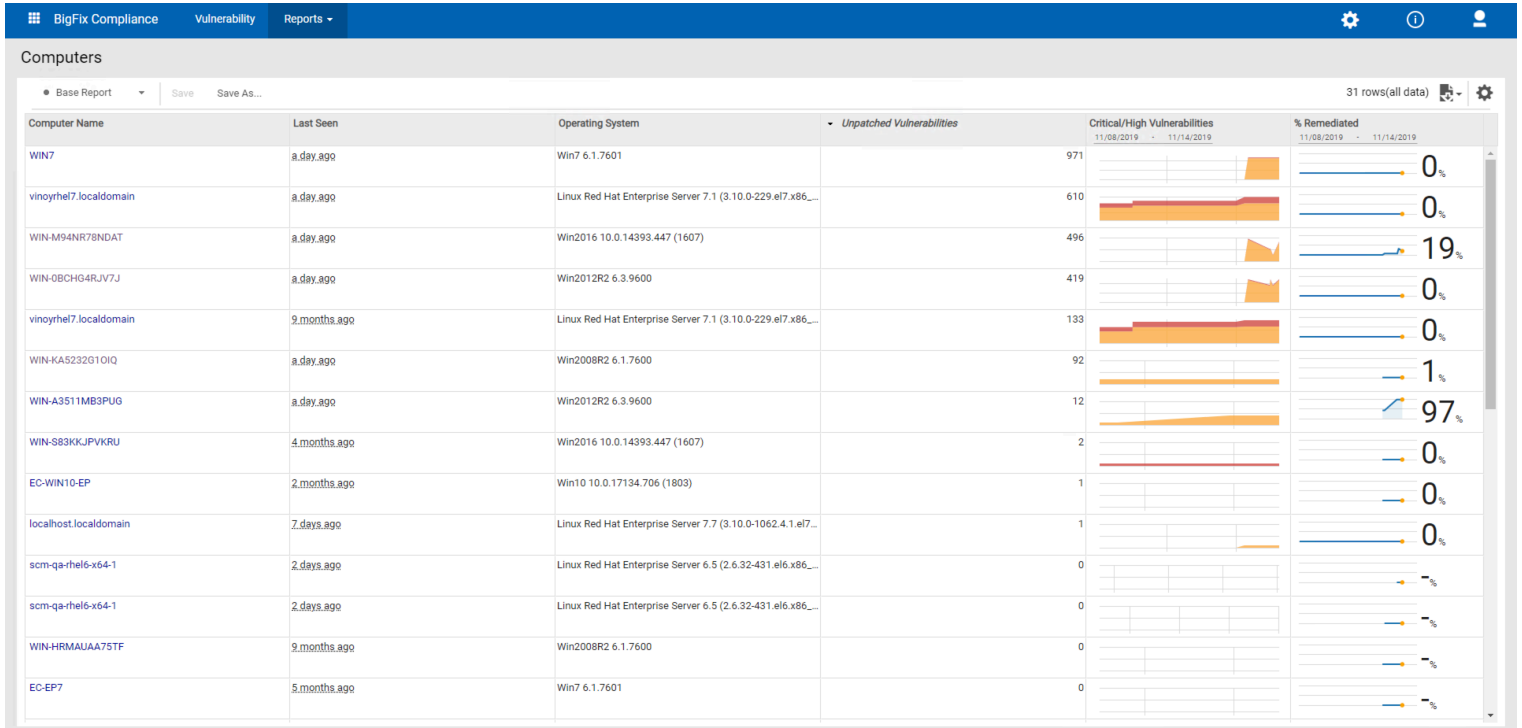


ID	Name	Fixlet ID	Severity	Category	Source	Source Release Date	Days Since Release
31243	MS19-AUG: Security Monthly Quality Rollup - Monthly Rollup - Windows Server 2008 SP2 - KB4512476 (x64) (Superseded)	451247601	Critical	Security Update	Microsoft	08/12/2019	94
31244	MS19-AUG: Security Monthly Quality Rollup - Monthly Rollup - Windows Server 2008 SP2 - KB4512476 (Superseded)	451247603	Critical	Security Update	Microsoft	08/12/2019	94
31248	MS19-AUG: Security Only Quality Update - Security Only - Windows Server 2012 - KB4512482 (x64)	451248201	Critical	Security Update	Microsoft	08/12/2019	94
31249	MS19-AUG: Security Only Quality Update - Security Only - Windows Server 2008 R2 SP1 - KB4512486 (x64)	451248601	Critical	Security Update	Microsoft	08/12/2019	94
31250	MS19-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4512486 (x64)	451248603	Critical	Security Update	Microsoft	08/12/2019	94
31251	MS19-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4512486	451248605	Critical	Security Update	Microsoft	08/12/2019	94
31252	MS19-AUG: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - KB4512488 (x64) (Superseded)	451248801	Critical	Security Update	Microsoft	08/12/2019	94
31253	MS19-AUG: Security Monthly Quality Rollup - Monthly Rollup - Windows Server 2012 R2 - KB4512488 (x64) (Superseded)	451248803	Critical	Security Update	Microsoft	08/12/2019	94
31254	MS19-AUG: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - KB4512488 (Superseded)	451248805	Critical	Security Update	Microsoft	08/12/2019	94
31255	MS19-AUG: Security Only Quality Update - Security Only - Windows Server 2012 R2 - KB4512489 (x64)	451248901	Critical	Security Update	Microsoft	08/12/2019	94
31256	MS19-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB4512489 (x64)	451248903	Critical	Security Update	Microsoft	08/12/2019	94
31257	MS19-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB4512489	451248905	Critical	Security Update	Microsoft	08/12/2019	94
31258	MS19-AUG: Security Only Quality Update - Security Only - Windows Server 2008 SP2 - KB4512491 (x64)	451249101	Critical	Security Update	Microsoft	08/12/2019	94
31259	MS19-AUG: Security Only Quality Update - Security Only - Windows Server 2008	451249103	Critical	Security Update	Microsoft	08/12/2019	94

HCL SOFTWARE

Computer List

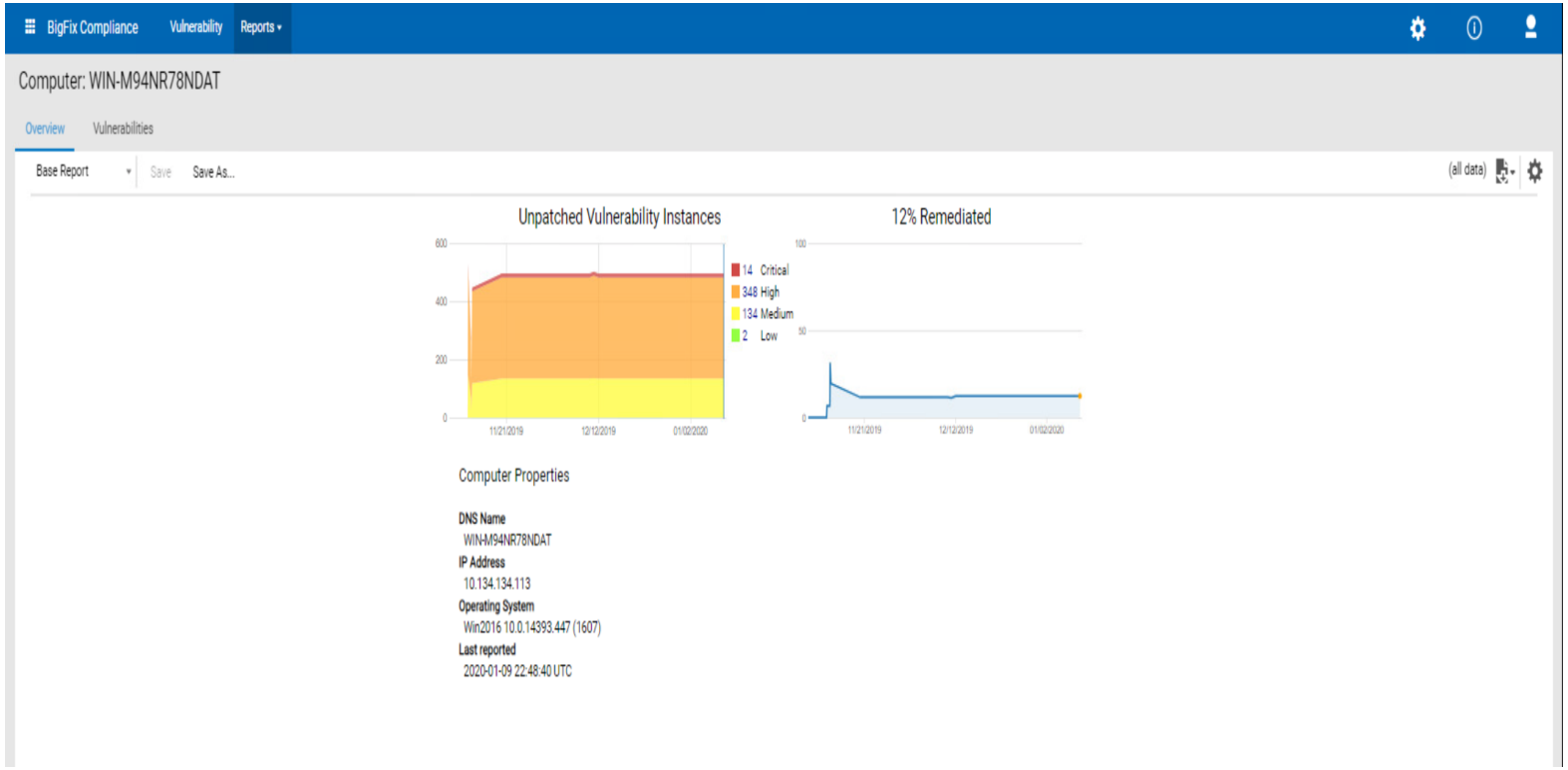
- All the computers being tracked
- Each computer's basic properties including last seen, OS, etc.
- The total number of unremediated vulnerabilities
- A trending of unremediated vulnerabilities in critical and high severities.
- A trending of the percentage of the vulnerabilities that have been remediated.
- Sorting all data based on vulnerability or remediation status to identify the 'riskiest' computers



HCL SOFTWARE

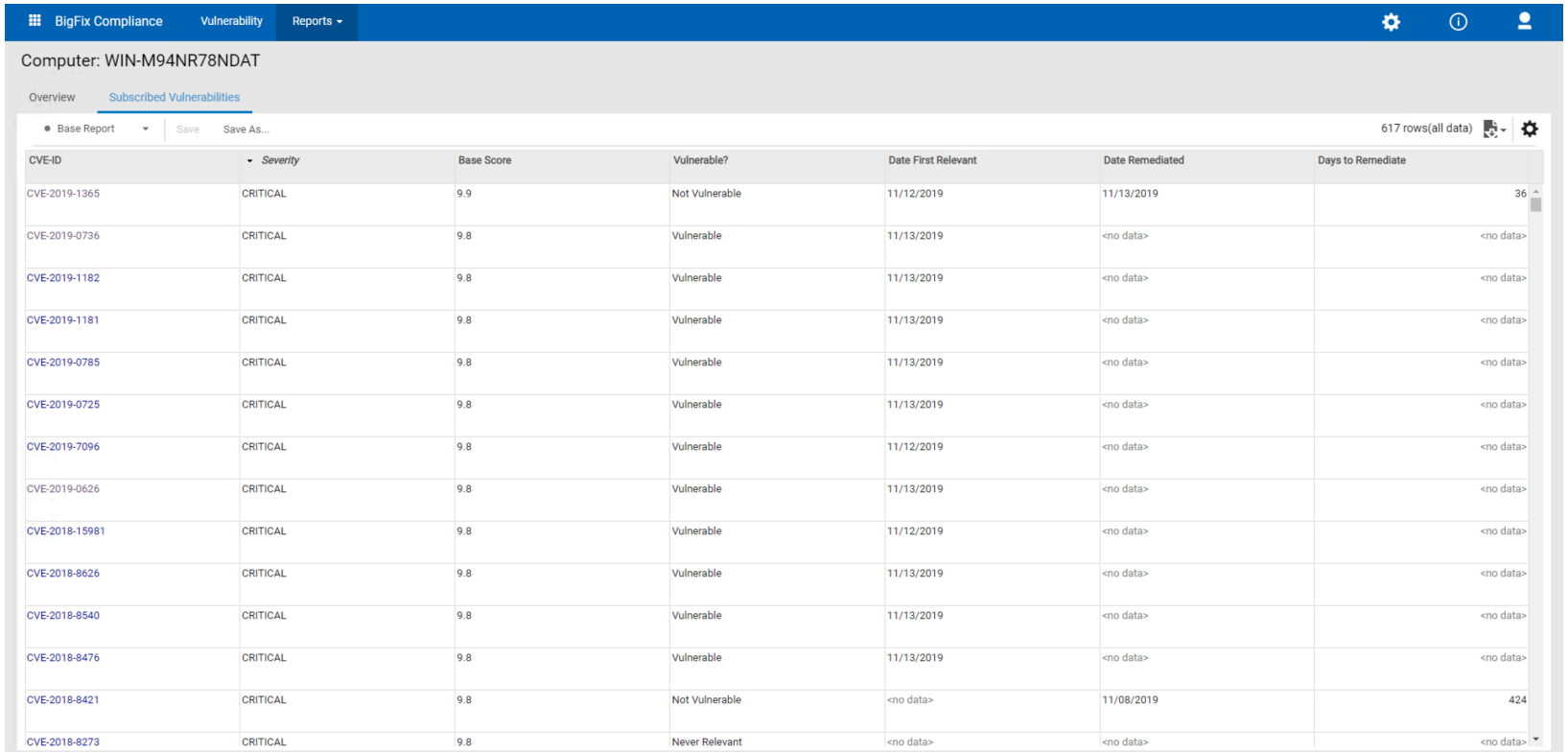
Computer Overview

- A trending of the total number of the unpatched vulnerabilities in each severity
- A trending of the vulnerabilities that have been remediated.
- Computer Details



Computer – Vulnerability Sub-report

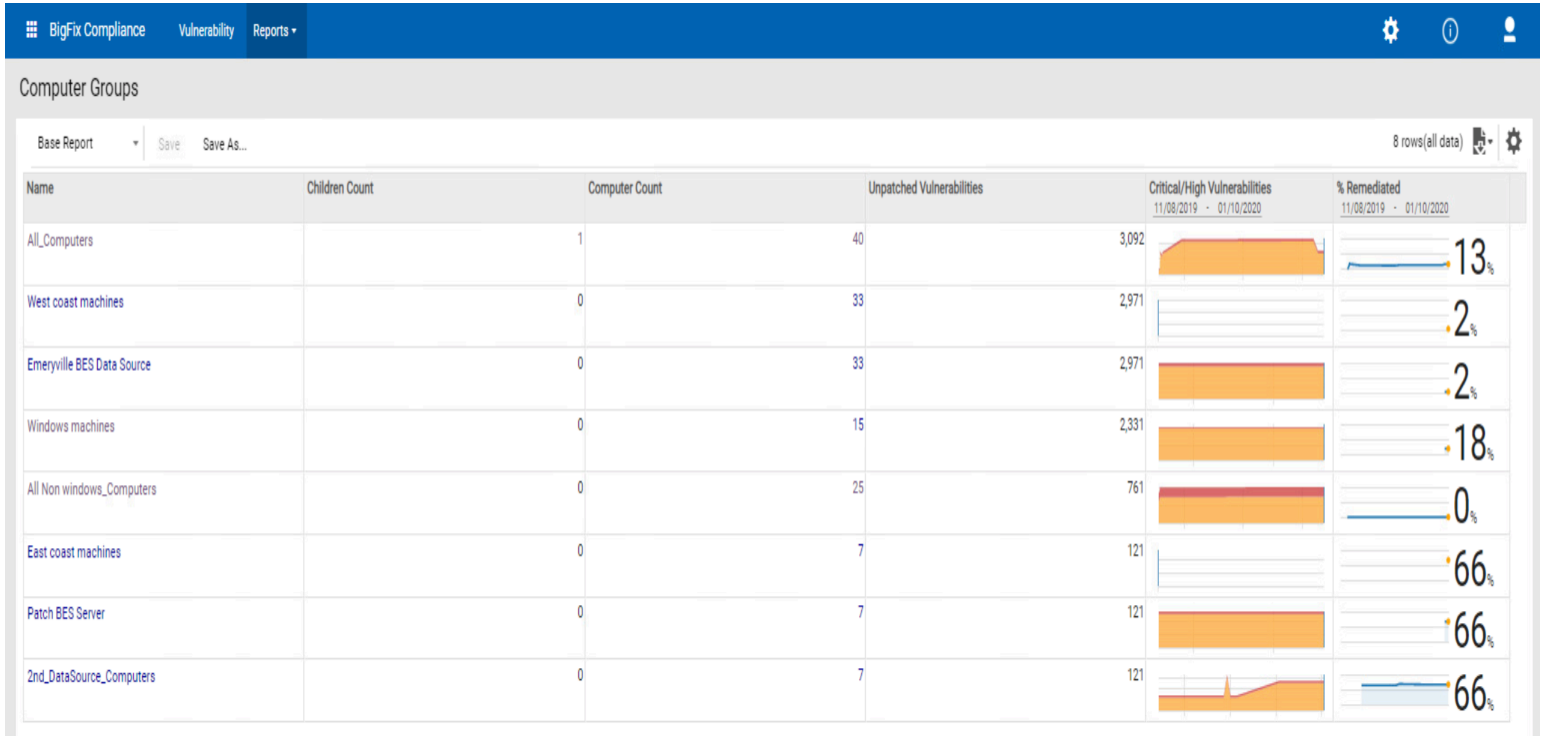
- All the vulnerabilities, either remediated or yet to be remediated
- Each vulnerability's (CVE) properties including severity, CVSS, whether it has been remediated, the date it was first reported
- If remediated, the date when it was remediated, and how long it took to remediate after first reported



CVE-ID	Severity	Base Score	Vulnerable?	Date First Relevant	Date Remediated	Days to Remediate
CVE-2019-1365	CRITICAL	9.9	Not Vulnerable	11/12/2019	11/13/2019	36
CVE-2019-0736	CRITICAL	9.8	Vulnerable	11/13/2019	<no data>	<no data>
CVE-2019-1182	CRITICAL	9.8	Vulnerable	11/13/2019	<no data>	<no data>
CVE-2019-1181	CRITICAL	9.8	Vulnerable	11/13/2019	<no data>	<no data>
CVE-2019-0785	CRITICAL	9.8	Vulnerable	11/13/2019	<no data>	<no data>
CVE-2019-0725	CRITICAL	9.8	Vulnerable	11/13/2019	<no data>	<no data>
CVE-2019-7096	CRITICAL	9.8	Vulnerable	11/12/2019	<no data>	<no data>
CVE-2019-0626	CRITICAL	9.8	Vulnerable	11/13/2019	<no data>	<no data>
CVE-2018-15981	CRITICAL	9.8	Vulnerable	11/12/2019	<no data>	<no data>
CVE-2018-8626	CRITICAL	9.8	Vulnerable	11/13/2019	<no data>	<no data>
CVE-2018-8540	CRITICAL	9.8	Vulnerable	11/13/2019	<no data>	<no data>
CVE-2018-8476	CRITICAL	9.8	Vulnerable	11/13/2019	<no data>	<no data>
CVE-2018-8421	CRITICAL	9.8	Not Vulnerable	<no data>	11/08/2019	424
CVE-2018-8273	CRITICAL	9.8	Never Relevant	<no data>	<no data>	<no data>

Computer Group List

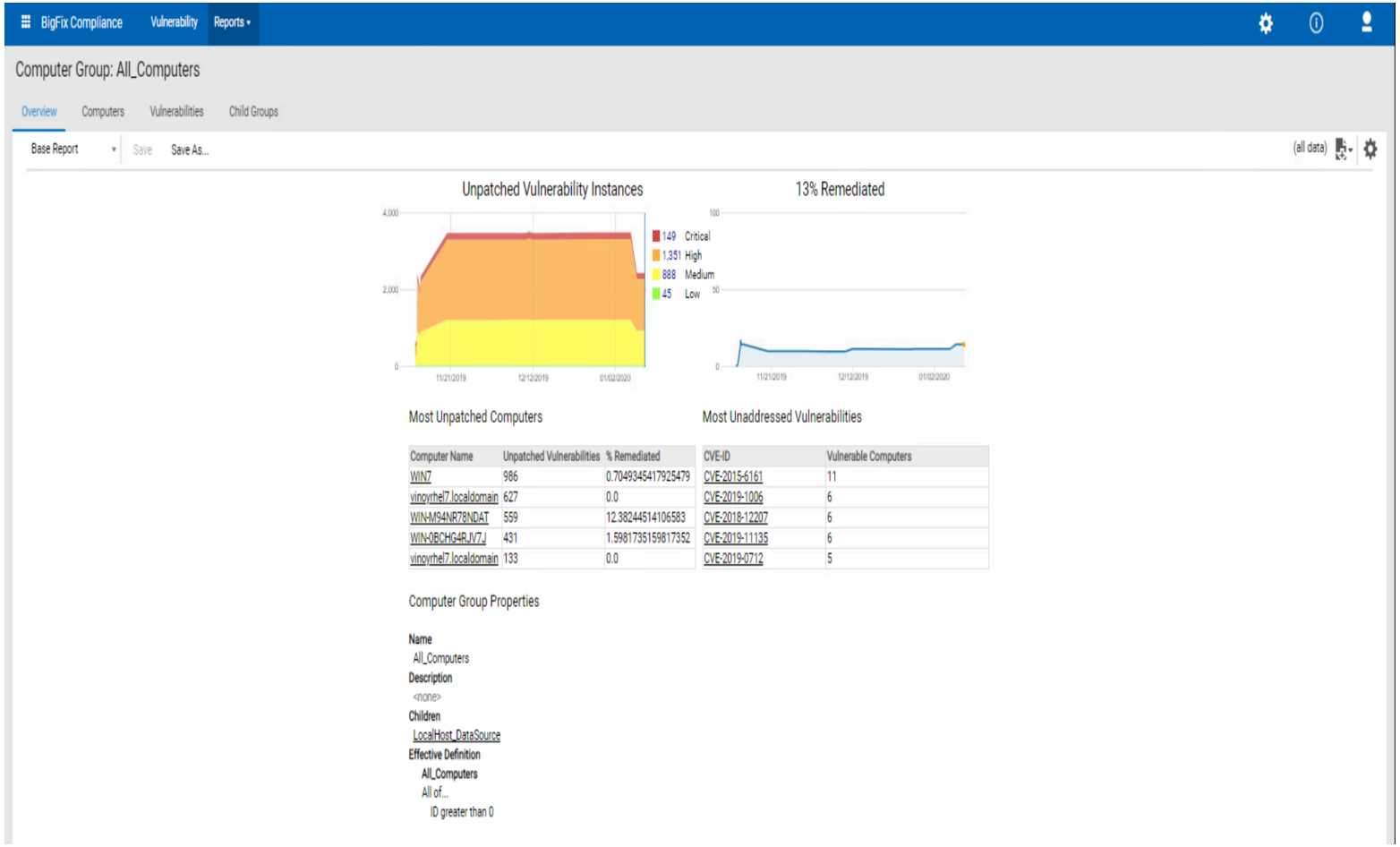
- All the computer groups that are defined in SCA
- The total number of unremediated vulnerabilities in a group
- A trending of unremediated vulnerabilities in critical and high severities.
- A trending of the percentage of the vulnerabilities that have been remediated.
- Sorting data based on vulnerability or remediation status to identify the ‘riskiest’ computer group



Name	Children Count	Computer Count	Unpatched Vulnerabilities	Critical/High Vulnerabilities 11/08/2019 - 01/10/2020	% Remediated 11/08/2019 - 01/10/2020
All_Computers	1	40	3,092		13%
West coast machines	0	33	2,971		2%
Emeryville BES Data Source	0	33	2,971		2%
Windows machines	0	15	2,331		18%
All Non windows_Computers	0	25	761		0%
East coast machines	0	7	121		66%
Patch BES Server	0	7	121		66%
2nd_DataSource_Computers	0	7	121		66%

Computer Group Overview

- A trending of the total number of the unpatched vulnerabilities in each severity
- A trending of the percentage of the vulnerabilities that have been remediated.
- The computers that have the greatest number of unpatched vulnerabilities
- The vulnerabilities that have not been addressed with the greatest number of computers



Survey / Feedback form

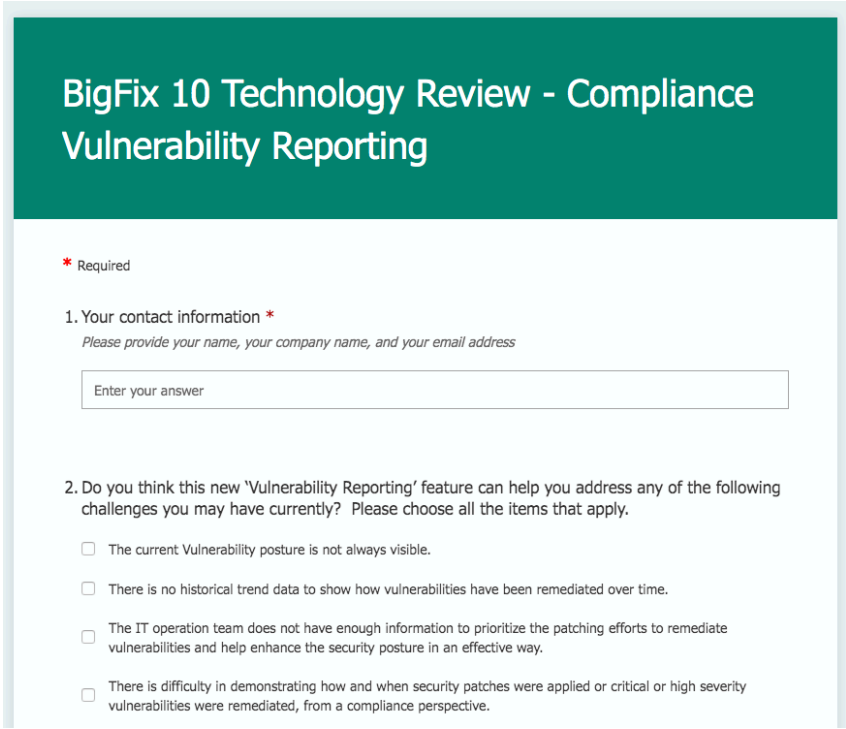
HCL SOFTWARE

Survey/feedback form

Open [BigFix 10 Technology Preview survey](#).

Complete this survey and click Submit to send your feedback to us.

Thank you for your participation in making BigFix better! Please feel free to reach out to Jason Honda (jason.honda@hcl.com) if you have any questions about or comments on the Technology Preview process.



BigFix 10 Technology Review - Compliance Vulnerability Reporting

* Required

1. Your contact information *

Please provide your name, your company name, and your email address

Enter your answer

2. Do you think this new 'Vulnerability Reporting' feature can help you address any of the following challenges you may have currently? Please choose all the items that apply.

- The current Vulnerability posture is not always visible.
- There is no historical trend data to show how vulnerabilities have been remediated over time.
- The IT operation team does not have enough information to prioritize the patching efforts to remediate vulnerabilities and help enhance the security posture in an effective way.
- There is difficulty in demonstrating how and when security patches were applied or critical or high severity vulnerabilities were remediated, from a compliance perspective.