U.S. DEPARTMENT OF LABOR

Office of Job Corps

Vulnerability Remediation/ Patch Deployment and Installation Guide

NOVEMBER 2018

Document Change History

Date	Filename/Version #	Author	Revision Description
11/12/2018	**Vulnerability Remediation/ Patch Deployment and Installation Guide**	**JCDC Security**	**Original**

Document Review History

Date	Version #	Reviewers
5/10/2016	**1.0**	**Sandra Steves**

Table of Contents

Contents

1 OVERVIEW

This document provides Job Corps Data Center's (JCDC's) procedures for addressing vulnerabilities within its IT environment.

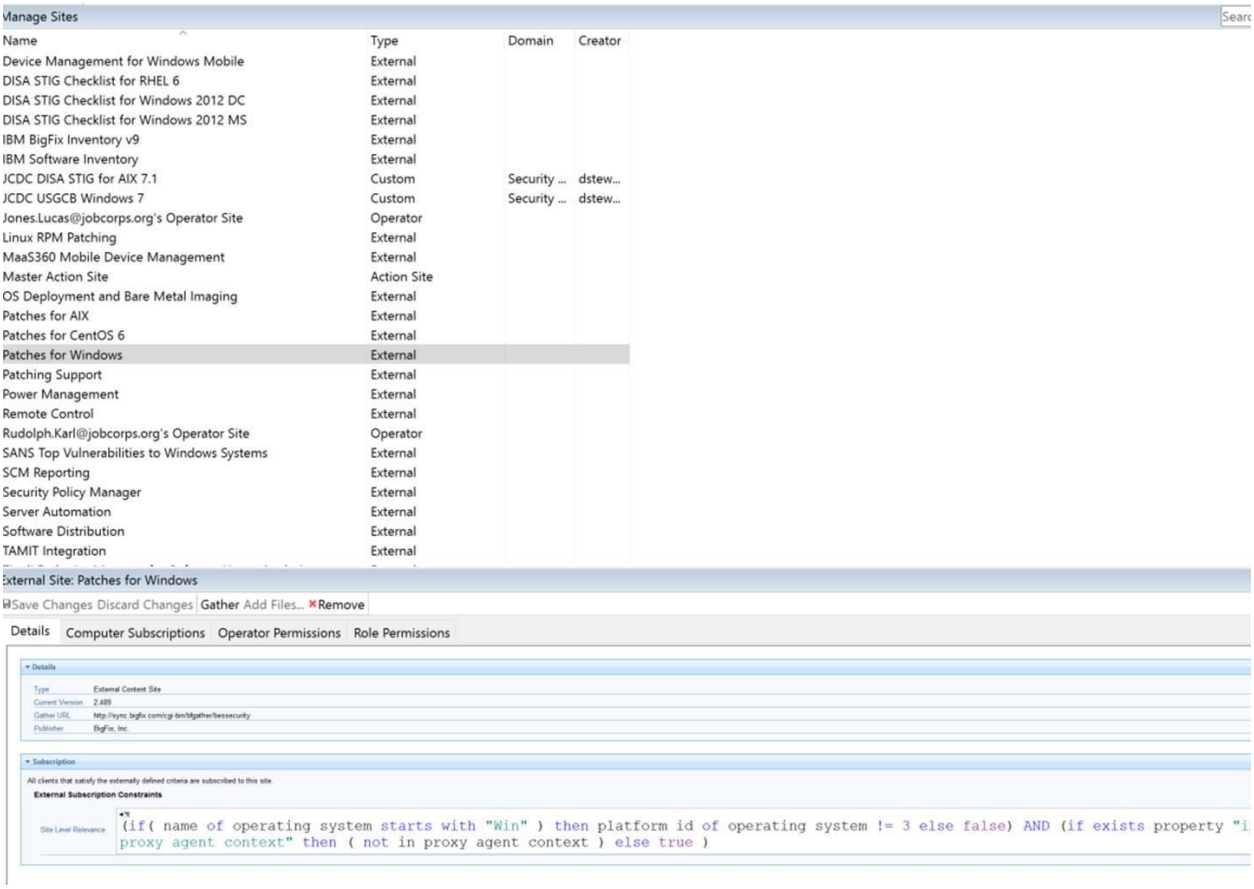
2 IDENTIFYING VULNERABILITIES

JCDC uses the **Tenable Nessus** tool to scan the entire JCDC network (via administrative credentials) for vulnerabilities such as missing security updates ("patches"), noncompliance with security standards, and exploitable information system entry and exit points. The Nessus tool allows JCDC to group devices for scans (e.g., JCDC Servers, Windows Servers, JCDC/MTAC Staff) and to schedule weekly or biweekly scans for those groups. The scans comprehend the network configuration, the website, and every device on the network.

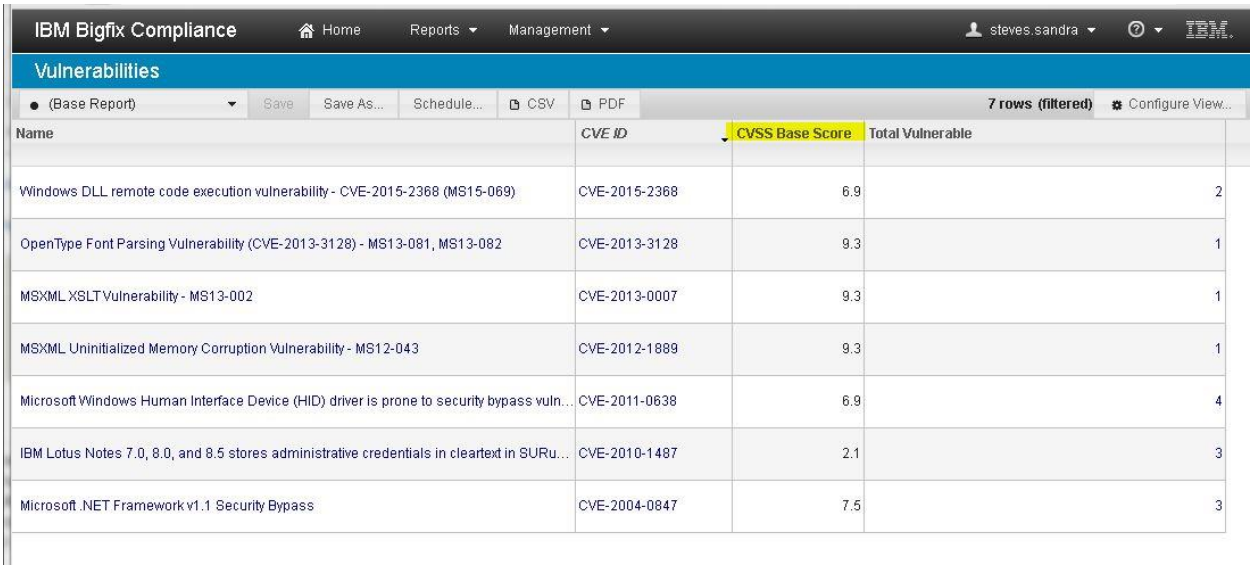
In addition, JCDC uses **IBM Tivoli Endpoint Manager** (aka "BigFix"), an agent-based software solution, to deploy and install patches for vulnerabilities in the Microsoft, Linux, and UNIX operating systems; for third-party software installed on JCDC devices; and for compliance with security standards. BigFix is included in the baseline configuration of all JCDC workstations, laptops, and servers and is thus able to scan all authorized devices on the network. JCDC subscribes to patch sources ("sites") provided through BigFix, and it also uses BigFix to install custom patches created with tools such as ForeScout and those provided for Google Chrome. In addition, JCDC uses BigFix to conduct continuous patch monitoring and reporting in real time.

JCDC follows the Common Vulnerability Scoring System (CVSS) for classifying vulnerabilities by severity. This system is also followed by Nessus and BigFix.

The following screenshot shows a list of sites/sources, and the constraints for Windows patches.



The following screenshot shows continuous vulnerability reporting in Bigfix.



JCDC also installs security updates based on **DOL security bulletins** requiring action. An example of a bulletin follows:

DOLCSIRC-N-16-110 VMware Releases Security Advisory

DOLCSIRC is distributing the following VMware Security Advisory.

Overview: As advised by US-CERT Alert on April 14, 2016, VMware released has released security updates to address a vulnerability in vCenter Server, vCloud Director, vRealize Automation Identity Appliance, and the Client Integration Plugin.

Description: The VMware Client Integration Plugin does not handle session content in a safe way. This may allow for a Man in the Middle attack or Web session hijacking in case the user of the vSphere Web Client visits a malicious Web site.

Impact: Exploitation of this vulnerability may allow a remote attacker to obtain sensitive information.

Software affected:

- vCenter Server 6.0 (any 6.0 version prior to 6.0 U2)
- vCenter Server 5.5 U3a, U3b, U3c
- vCloud Director 5.5.5
- vRealize Automation Identity Appliance 6.2.4

Solution: Follow the Agency's policy and standard protocols, review the security bulletin, test, and timely implement the security updates.

References:

- https://www.us-cert.gov/ncas/current-activity/2016/04/14/VMWare-Releases-Security-Updates
- http://www.vmware.com/security/advisories/VMSA-2016-0004.html

CVE's: CVE-2016-2076

Required Actions:

1) Agencies are to review VMware Security Advisory VSMA-2016-0004 and apply the necessary updates.
2) Agencies must report the level of impact of their systems and apply the recommended updates and/or patches or workaround as required.
3) Whether agency is impacted or not, please report back to DOLCISRC by April 19, 2015.

3 PATCH INSTALLATION

When vulnerabilities are identified, they are patched as expeditiously as possible. The Department of Labor's Office of the Chief Information Officer (DOL-OCIO) has issued the following parameters for security update installation and vulnerability remediation:

Security update (patch) criticality	Installation schedule
Critical	within 72 hours of release
High	within 1 business week of release
Moderate	within 30 business days of release
Low	within 60 business days of release

Vulnerability criticality	Remediation schedule
Critical	within 5 business days of discovery
High	within 10 business days of discovery
Moderate	within 30 business days of discovery
Low	within 60 business days of discovery

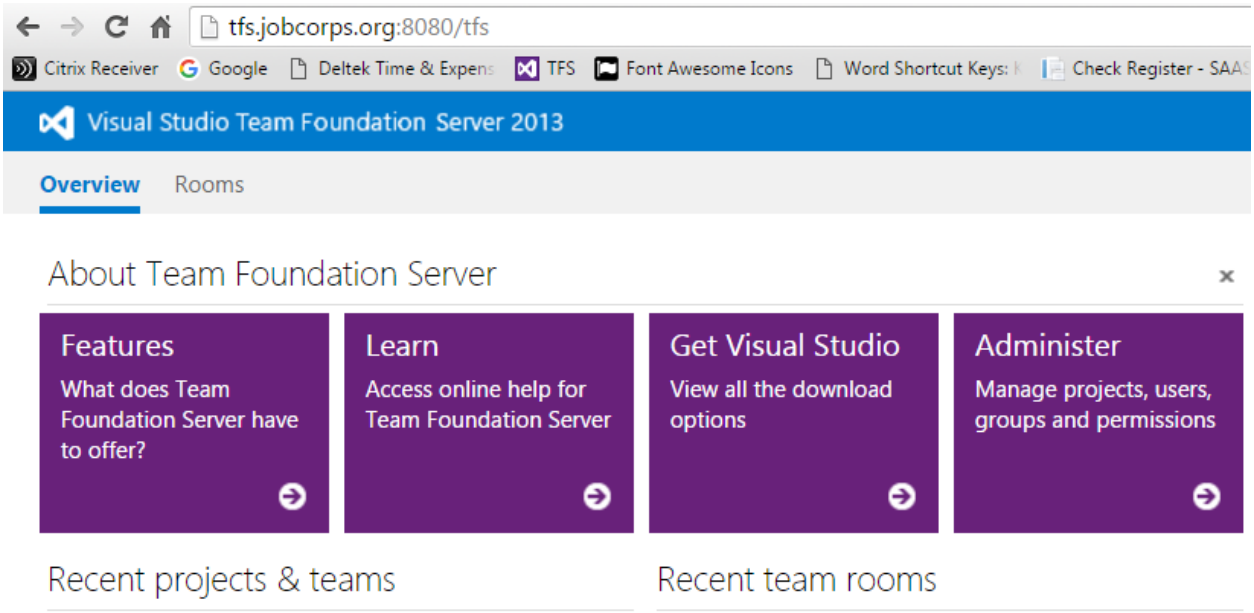
Patch installation and vulnerability remediation constitute changes that must undergo standard JCDC Change Management procedures. These are as follows.

3.1 CREATE A WORK ITEM FOR THE SECURITY UPDATE.

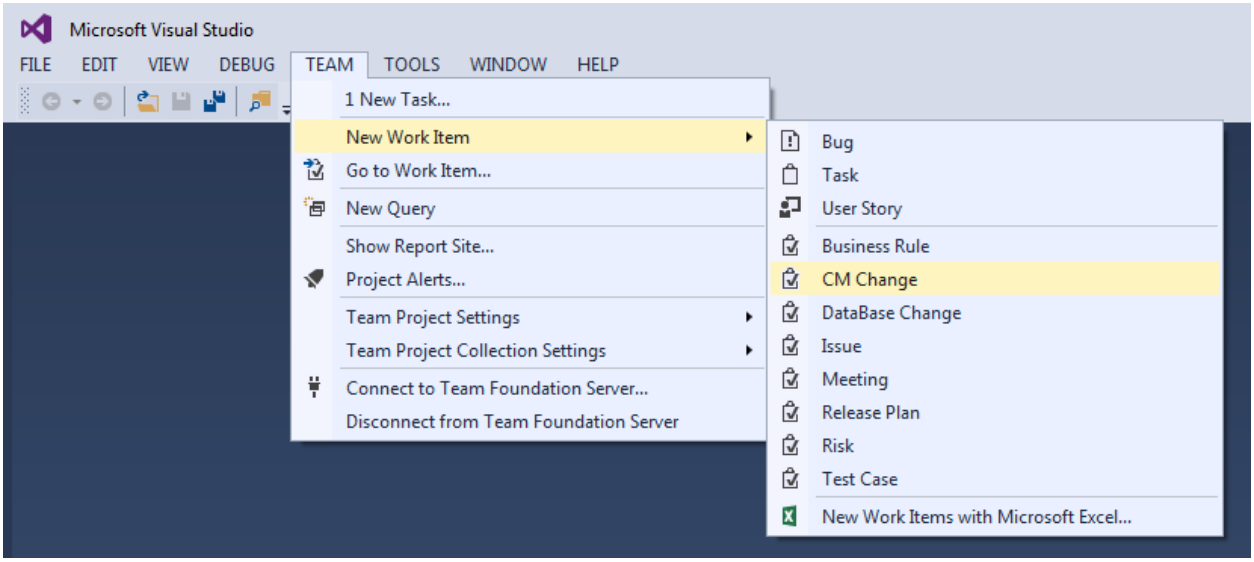
Action	Role or Group
1. Create a Work Item for the update, providing details from start to completion, in Team Foundation Server (TFS) and send to Configuration Management (CM) manager	Network System Admin and/or JCDC Security Personnel

JCDC's implementation of TFS includes both web and Microsoft Visual Studio access.

Web:



Visual Studio:



The following screenshot provides an example of Change Control board action in response to a DOL Security Bulletin:

1. **Project Name:** DOLCSIRC-N-15-109 Microsoft Security Bulletin (MS15-078) *(WI#11757)*
2. **Owner:** Derek Stewart
3. **Reason for change:**

DOLCSIRC-N-15-109 Microsoft Security Bulletin (MS15-078)
DOLCSIRC is distributing the following Microsoft Security Bulletin Notification.

Overview: Microsoft has released a security update to address a critical vulnerability in Windows. The vulnerability could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains embedded OpenType fonts.

Description: As advised by US-CERT Alert, on July 20, 2015, Microsoft has released a security update to address a critical vulnerability in Windows. The security update addresses the vulnerability by correcting how the Windows Adobe Type Manager Library handles OpenType fonts.

Impact: Exploitation of this vulnerability may allow a remote attacker to take control of an affected system.

Systems Affected:

- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8 and Windows 8.1
- Windows Server 2012 and Windows Server 2012 R2
- Windows RT and Windows RT 8.1

Note: Please pay particular attention to notes in the MS Security Bulletin.

Solution: Follow the Agency's policy and standard protocols, review the security bulletin, test, and timely implement the security updates. Further required actions are provided below.

References:
https://www.us-cert.gov/ncas/current-activity/2015/07/20/Microsoft-Releases-Security-Update
https://technet.microsoft.com/en-us/library/security/MS15-078
CVE's: CVE-2015-2426

Required Actions:

Agencies need to review Microsoft Security Bulletin (MS15-078) to determine if they are impacted; Agencies must report the level of impact of their systems and apply the recommended updates and/or patches or workaround as required. Whether agency is impacted or not, please report back to DOLCSIRC by COB July 23, 2015.

3.2 TEST THE SECURITY UPDATE.

Action	Role or Group
2. CM promotes Work Item	CM manager
3. Integrate the Patch in test environment	Network System Admin
4. Test the Patch	Network System Admin

The test environment has test servers representing all mission-critical applications. Ideally, every type of platform in the enterprise is represented in the test environment. When it is not possible to maintain a test environment that mirrors the production environment, updates are installed on the least critical, most easily recoverable servers first. These are servers without a lot of data or applications that will need to be restored, such as print servers.

The level of testing depends on risk to the information system and the priority of the update as determined by the Patch Vulnerability Group. Security updates are tested for effectiveness and potential side effects on Job Corps information systems prior to installation in production environments, and then installed on all machines as appropriate except where instances preclude system functionality.

In addition, each group of system administrators performs testing according to group practices.

The **CitrixAdmins** group is responsible for the following devices, and tests as follows:

CITRIX DESKTOP

1. Updates are applied to the QA-QC Desktop; QA is notified and looks for any issues.
2. Upon success, updates are applied to 10–20 servers in Production.

WEB SERVERS

1. JCDev and QA servers are configured to get updates automatically; script notifies Dev and QA when systems are rebooted with what patches
2. Upon success, regression occurs on the QC image the week and a half prior to the scheduled promote date.

WORKSTATIONS

1. Updates are pushed to vlan6 to network security workstations; systems are rebooted and monitored.
2. Updates are pushed to all JCDC workstations; systems are rebooted and monitored.

The **UnixAdmins** group is responsible for the following devices, and tests as follows:

1. Updates are applied to 2 test systems with AIX 6.1 (oldntp, rmaster2) and 1 system with AIX 7.1 (richsys3).
2. Upon success, updates are applied to non-database systems (vmaster, jcdcrs15, jcdcntp).
3. Upon success, patches are applied to DEV/QA systems with Sybase databases active (jcdcrs3, jcdcrs4, jcdcrs6, jcdcrs10, jcdcrs11) to make sure that they don't break the Sybase environment.

4. Upon success, patches are applied to production systems with Sybase (jcdcrs5, jcdcrs7, richsys1, richsys2, richsys8).

The **SecurityAdmins** group is responsible for the following devices, and tests as follows:

1. Security updates are installed on Linux security servers within 24 hours of release.
2. Upon success, updates are installed on other Windows servers.

The **JCDCDBAAdmins** group is responsible for the following devices, and tests as follows:

1. Windows patches are installed on Dev/QA and proof-of-concept SQL servers and Sybase IQ servers.
2. Upon success, updates are scheduled for the remaining machines (i.e., production). SQL servers are patched during Sybase/UNIX downtime to minimize impact on users.

Testing periods before updates are installed in production are as follows:

Security update (patch) importance	(Maximum) testing duration prior to production install
Critical	48 hours
High	48 hours
Moderate	48 hours
Low	1 month

A Work Item reflecting steps 2-4 (promotion, integration in test environment, and testing) is shown here:

Operations Change Request 7115

- ID 7115
- Netbackup upgrade from 7.5.0.7 to 7.6.0.1

Status

- Assigned To Simon Medrano
- State Proposed

Classification

- Area Operations
- Iteration Operations

History

1/22/2015 8:58:50 AM Edited by Simon Medrano

1/22/2015 8:55:46 AM Edited by Simon Medrano

1/21/2015 3:03:59 PM Created by Simon Medrano

An update to Netbackup version 7.5.0.7 is needed in order to install the new hardware appliances model 5230, the new version needs to be at Netbackup 7.6.0.1.

A ticket will be opened with Symantec Tech support services during the update in case it is needed.

Reason

New Symantec Appliances model 5230 are being installed in order to support data replication between sites, it is recommended that the Netbackup environment version be upgraded from 7.5.0.7 to 7.6.0.1.

Notes

TESTER NOTES

Upgrade path is very similar to previous version updates of Netbackup software, we have tested these in the past, see CR#32898 for more information.

01-22-2015- Testing has been done successfully on a standalone "Test server" where Netbackup 7.5.0.7 was previously installed.

3.3 CONDUCT A SECURITY IMPACT ANALYSIS.

Action	Role or Group
5. Conduct a Security Impact Analysis (SIA), which is attached to the TFS Work Item	Compliance Administrator Security Compliance Manager

This process must be documented; upon completion, the documentation is archived.

A Security Impact Analysis worksheet is shown here:

Security Impact Analysis Worksheet

Change or Revision #	WI #7115
Date of Security Impact Analysis (SIA):	1/22/2015
Analysis Performed By:	Sandra Steves
Platform:	Infrastructure
Component Specifications:	Netbackup
Describe affects of the change (i.e. Baseline Changes, Security Risks, System Changes):	An update to Netbackup version 7.5.0.7 is needed in order to install the new hardware appliances model 5230, the new version needs to be at Netbackup 7.6.0.1.
Overall Potential Impact to Security?	☒ N/A ☐ Low ☐ Medium ☐ High
Explanation of Security Impact:	Updating Netbackup should improve the JC security posture (see #10).

NIST 800-53 Security Controls

1. Access Control Will change(s) to system effect how the system limits: (i) Information system access to authorized users, processes acting on behalf of authorized users or devices; and (ii) the types of transactions and functions that authorized users are permitted to exercise?
☒ **No** ☐ **Yes (If Yes, please describe below)**
2. Security Awareness Will change(s) affect required system training to ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities?
☒ **No** ☐ **Yes (If Yes, please describe below)**
3. Audit and Accountability Will change(s) affect how system audit requirements to (i) create, protect, and retain information system audit records to the extend needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions?
☒ **No** ☐ **Yes (If Yes, please describe below)**
4. Configuration Management Will change(s) to the system impact the (i) baseline configuration and inventory of organizational information systems: (ii) establishment and enforcement of security configuration settings; and (iii) ability to monitor and control changes to the baseline configurations and to the constituent components of the systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycle?
☒ **No** ☐ **Yes (If Yes, please describe below)**

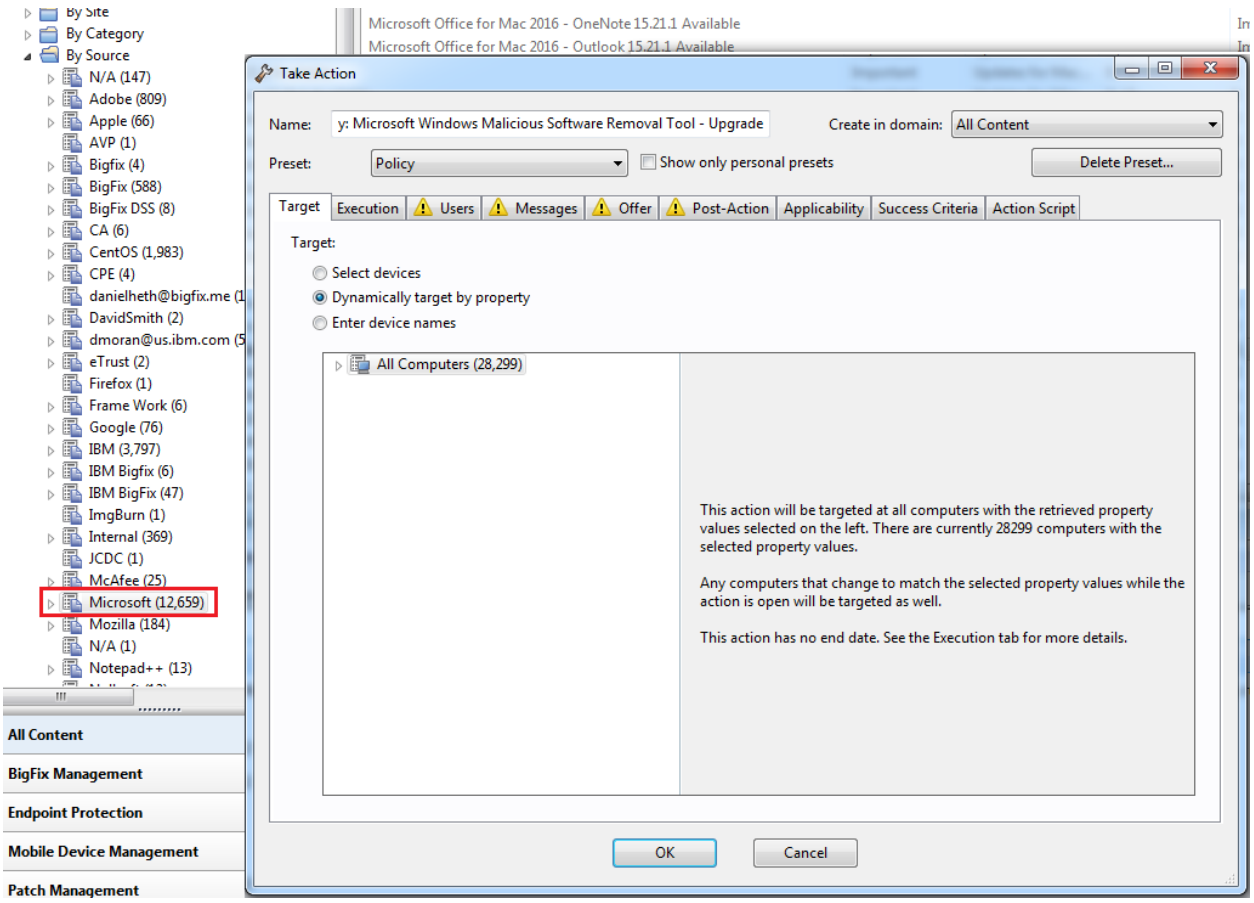
3.4 OBTAIN MANAGEMENT APPROVAL FOR THE SECURITY UPDATE.

Action	Role or Group
6. CM distributes the Work Item to managers for approval	CM manager
7. Managers approve	CCB board members
8. Final approval	IT Director

Approvals are obtained via email, which are archived by the CM manager.

Action	Role or Group
9. Deploy the Patch	Network System Admin or JCDC Security Personnel
10. Verify the Patch/Vulnerability Remediation Deployment and Installation	Network System Admin or JCDC Security Personnel
11. Verify Deployment Using Vulnerability Scanning	Network System Admin or JCDC Security Personnel
12. Update Documentation	CM manager and all managers whose groups will be affected, to potentially include: • Technical Assistance Center (TAC) Manager • Security Compliance Manager • Software Quality Assurance Manager • Operations & DB Manager • Network Manager • Software Development Manager • Training Manager

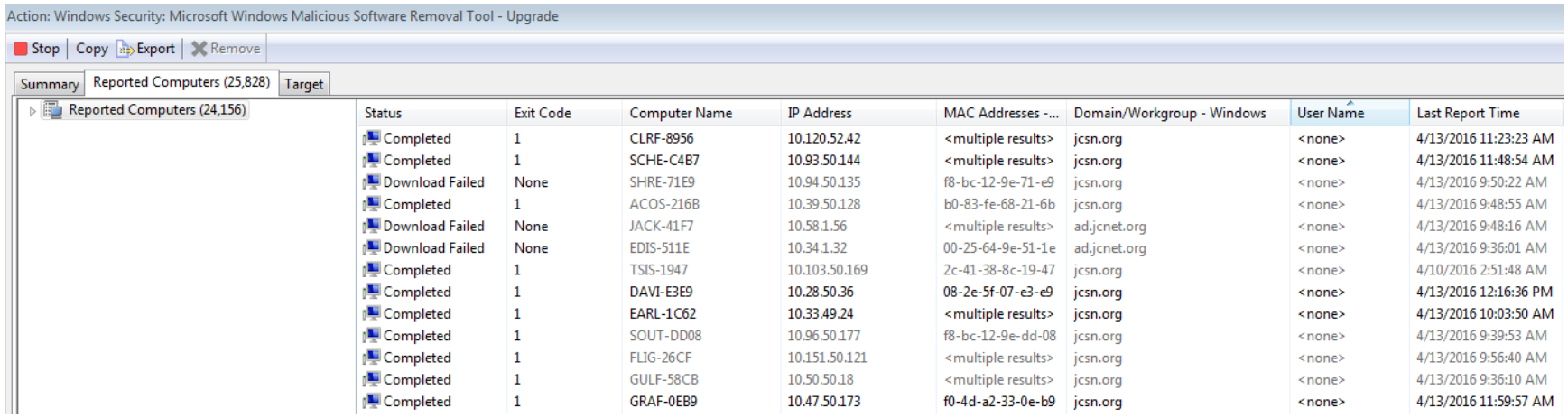
BigFix is used to deploy and install security updates. In the screenshot below, Microsoft patches will be installed on all affected systems:



The Patch Vulnerability Group updates Nessus and BigFix to reflect new configurations and testing for old configurations. Verification methods meet the following criteria:

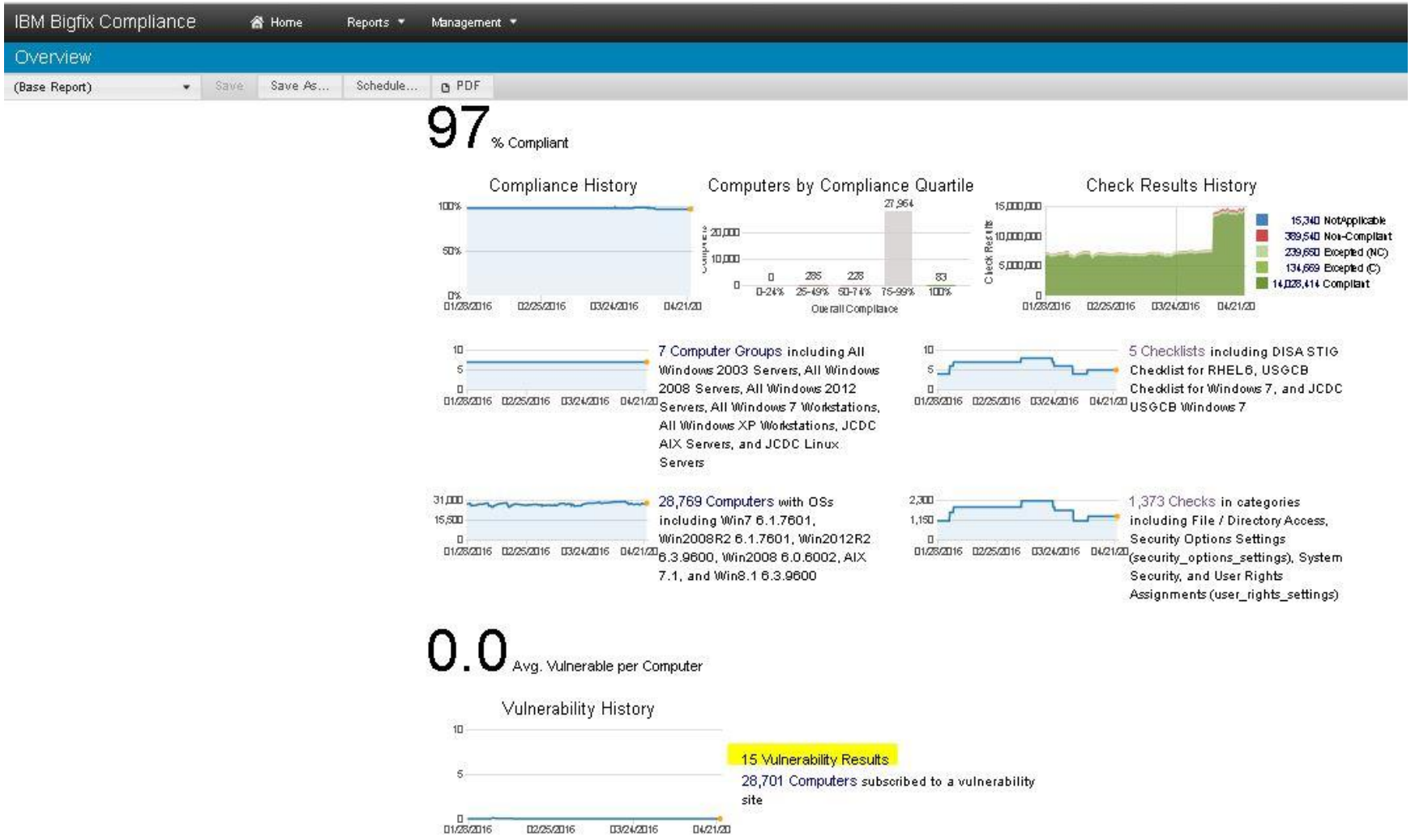
- The files or configuration changes the remediation was intended to correct are verified as stated in the vendor's documentation.
- The host is scanned with a vulnerability scanner capable of detecting known vulnerabilities.
- Logs are reviewed to verify the recommended security updates were installed properly.
- Verification does not utilize exploit procedures (including, but not limited to, a penetration test); and the code does not exploit any vulnerabilities without authorization and approval from the information system's authorizing official.

BigFix verifies updates as they are pushed out in real time:



Status	Exit Code	Computer Name	IP Address	MAC Addresses -...	Domain/Workgroup - Windows	User Name	Last Report Time
Completed	1	CLRF-8956	10.120.52.42	<multiple results>	jcsn.org	<none>	4/13/2016 11:23:23 AM
Completed	1	SCHE-C4B7	10.93.50.144	<multiple results>	jcsn.org	<none>	4/13/2016 11:48:54 AM
Download Failed	None	SHRE-71E9	10.94.50.135	f8-bc-12-9e-71-e9	jcsn.org	<none>	4/13/2016 9:50:22 AM
Completed	1	ACOS-216B	10.39.50.128	b0-83-fe-68-21-6b	jcsn.org	<none>	4/13/2016 9:48:55 AM
Download Failed	None	JACK-41F7	10.58.1.56	<multiple results>	ad.jcnet.org	<none>	4/13/2016 9:48:16 AM
Download Failed	None	EDIS-511E	10.34.1.32	00-25-64-9e-51-1e	ad.jcnet.org	<none>	4/13/2016 9:36:01 AM
Completed	1	TSIS-1947	10.103.50.169	2c-41-38-8c-19-47	jcsn.org	<none>	4/10/2016 2:51:48 AM
Completed	1	DAVI-E3E9	10.28.50.36	08-2e-5f-07-e3-e9	jcsn.org	<none>	4/13/2016 12:16:36 PM
Completed	1	EARL-1C62	10.33.49.24	<multiple results>	jcsn.org	<none>	4/13/2016 10:03:50 AM
Completed	1	SOUT-DD08	10.96.50.177	f8-bc-12-9e-dd-08	jcsn.org	<none>	4/13/2016 9:39:53 AM
Completed	1	FLIG-26CF	10.151.50.121	<multiple results>	jcsn.org	<none>	4/13/2016 9:56:40 AM
Completed	1	GULF-58CB	10.50.50.18	<multiple results>	jcsn.org	<none>	4/13/2016 9:36:10 AM
Completed	1	GRAF-0EB9	10.47.50.173	f0-4d-a2-33-0e-b9	jcsn.org	<none>	4/13/2016 11:59:57 AM

BigFix Compliance Analytics also reports on vulnerabilities in real time:



5 DOCUMENTATION

When the previous steps are complete, the Patch Vulnerability Group updates the inventory and notifies stakeholders when the security update installation is complete.

The following screenshot shows a snip of the Software Version Matrix maintained by the Configuration Manager:

Applications	QA/Test	Production/Prodtest/Training/RICHS
CaseNotes (2008)	No new release in QA	03.14.0096 (promoted: 12.17.2015)
CaseNotes3G (2012)	No new release in QA	03.19.0119 (promoted: 06.25.2015) – 2003 03.20.0120 (promoted: 08.27.2015) – 2012R2
CIS (2008)		02.80.0600c (promoted: 12.17.2015)
CIS3G (2012)	03.43.0443 (qa: 03.30.2016) 03.43.0444 (qa: 04.11.2016) 03.43.0445 (qa: 04.19.2016) 03.43.0446 (qa: 05.02.2016) 03.43.0447 (qa: 05.04.2016)	03.42.0442 (promoted: 03.31.2016)
CIS3G_HSD (2012)	03.01.0001 (qa: 11.24.2015) 03.01.0002 (qa: 12.07.2015)	
CIS3G_Payroll (2012)	03.01.0001 (qa: 09.28.2015) 03.01.0002 (skipped) 03.01.0003 (qa: 12.01.2015) 03.01.0004 (qa: 03.29.2016)	
CIS3G_Gary (2012)		Same as CIS3G
CISCasenotes	-- not being used in QA	01.01.0003 (promoted: 06.01.2011)
CSCAN (Scanner)	03.01.0005 (qa: 11.14.2012) - removed 11.26.2012	03.01.0004 (promoted: 11.02.2012)
CIS2SPAMIS (2008)	No new release in QA	02.01.0031h (promoted: 02.25.2016)
CSSET (2012)	No new release in QA	02.01.0001 (promote 02.25.2016)
CTS (2008)	No new release in QA	02.45.0182 (promoted: 01.07.2016)
CTS3G (2008)	No new release in QA	03.05.0063 (promoted: 04.28.2016)
DSS	01.01.0119 (qa: 08.15.2013)	01.11.0118 (promoted: 08.01.2013)
DSSREPORT	No new release in QA	01.10.0098 (promoted: 07.31.2015)
EFolder (2012,2008)	No new releases in QA	03.05.0033 (promoted: 10.29.2015)
EFRG3G	03.01.0001 (qa: 08.21.2014) 03.01.0002 (qa: 09.04.2014)	
EIS/EIS3G (2012)	No new release in QA	03.16.0275 (promoted: 01.28.2016)
EPMS	No new release in QA	02.22.0111 (promoted: 04.17.2009)
EPMS3G (2012)	No new release in QA	03.07.0063 (promoted: 10.29.2015)

The full document is inserted here:

SW_Version_Matrix.docx

The Configuration Manager notifies stakeholders by email, as shown below:

From: Mike Ramos
Sent: Thursday, April 28, 2016 10:08 PM
To: JCEX JCDCSTAFF <JCEXJCDCSTAFF@jobcorps.org>
Subject: CDSS Promote to Production

The following have been promoted to Production, Prodtest, and Training:

- CTS3G 03.05 (JCDC Notice 15-181 New Release of CTS Sent out on 4/28/2016)
- FMS3G 03.11 (JCDC Notice 15-182 New Release of FMS3G Sent out on 4/28/2016)
- JCRL3G 03.02 (JCDC Notice 15-180 New Release of JCRL Sent out on 4/28/2016)
- STS 02.02 (moved to a 2012 Windows Server)
- STSE 02.02 (moved to a 2012 Windows Server)
- Help File Updates to CTS3G
- Help File Updates to FMS3G
- AMS Monthly Data for May 2016

Thanks!

Mike Ramos
Configuration Management