Vulnerability Assessment & Compliance Report

Table of Contents

Report Generated on: 4/3/2017 5:06 PM
Services provided by: Innovative Computer Systems

Vulnerability Assessment & Compliance Report

1 Overview

Office Location: xxxx

This following report is to collect supporting evidence used for the Security Risk Assessment & Compliance reporting as required by the U.S. Department of Health and Human Services. Risk Analysis reviews are performed yearly and/or unless there are significant changes to the administrative, physical or technical safeguards. As part of a risk analysis review, the organization must identify and document potential threats and vulnerabilities as stated below:

Identify and Document Potential Threats and Vulnerabilities

Organizations must identify and document reasonably anticipated threats to e-PHI. (See 45 C.F.R. §§ 164.306(a)(2) and 164.316(b)(1)(ii).) Organizations may identify different threats that are unique to the circumstances of their environment. Organizations must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Assess Current Security Measures

Organizations should assess and document the security measures an entity uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

The security measures implemented to reduce risk will vary among organizations. For example, small organizations tend to have more control within their environment. Small organizations tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard e-PHI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of e-PHI in a small organization may differ from those that are appropriate in large organizations.[7]

More information can be found at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

Vulnerability Assessment & Compliance Report

2 Scan Results

2.1 Identified Devices

The devices below have been identified during this vulnerability scan and are presented in the table below.

IP	FQDN	Operating System	Computer Name	MAC Address
x.x.x.x		Dell iDRAC		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	SERVER NAME	xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 2.6		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	SERVER NAME 1	xx:xx:xx:xx:xx
x.x.x.x		VMware ESXi		xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 2.2 Linux Kernel 2.4 Linux Kernel 2.6		xx:xx:xx:xx:xx
x.x.x.x		HP Integrated Lights Out		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows Server 2008		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows Server 2003 R2 Service Pack 2		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows Server 2008 R2		xx:xx:xx:xx:xx
x.x.x.x		Dell iDRAC		xx:xx:xx:xx:xx
x.x.x.x		Dell Remote Access Controller		xx:xx:xx:xx:xx
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 2.2 Linux Kernel 2.4 Linux Kernel 2.6		xx:xx:xx:xx:xx
x.x.x.x		Dell iDRAC		xx:xx:xx:xx:xx
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 2.6		xx:xx:xx:xx:xx

Vulnerability Assessment & Compliance Report

IP	FQDN	Operating System	Computer Name	MAC Address
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 8.1 Pro		xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 3.0 on Ubuntu 12.04 (precise)		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows Vista Microsoft Windows Server 2008 Microsoft Windows Server 2008 R2 Microsoft Windows 7		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows Vista Microsoft Windows Server 2008 Microsoft Windows Server 2008 R2 Microsoft Windows 7		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 2.4		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x				xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 2.2 Linux Kernel 2.4 Linux Kernel 2.6		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx

Vulnerability Assessment & Compliance Report

IP	FQDN	Operating System	Computer Name	MAC Address
x.x.x.x		Linux Kernel 3.0 on Ubuntu 12.04 (precise)		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional		xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 3.0 on Ubuntu 12.04 (precise)		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 3.0 on Ubuntu 12.04 (precise)		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Microsoft Windows 7 Professional Service Pack 1		xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 3.0 on Ubuntu 12.04 (precise)		xx:xx:xx:xx:xx
x.x.x.x		Linux Kernel 2.6		xx:xx:xx:xx:xx

There are **57 devices** identified during this scan.

2.2 Vulnerabilities Assessment Results

2.2.1 Overview

The table below displays the number of vulnerabilities identified for each device.

IP	Critical	High	Medium	Low
x.x.x.x	0	0	1	0
x.x.x.x	0	0	0	0
x.x.x.x	3	96	10	4
x.x.x.x	0	17	8	2
x.x.x.x	0	0	0	0
x.x.x.x	0	0	0	0
x.x.x.x	0	10	3	0
x.x.x.x	0	12	8	2
x.x.x.x	0	0	0	0
x.x.x.x	0	0	4	0

Vulnerability Assessment & Compliance Report

IP	Critical	High	Medium	Low
x.x.x.x	8	176	45	6
x.x.x.x	7	154	37	5
x.x.x.x	0	0	6	1
x.x.x.x	0	1	2	1
x.x.x.x	10	139	42	6
x.x.x.x	6	18	7	0
x.x.x.x	0	0	0	0
x.x.x.x	8	120	29	5
x.x.x.x	3	109	19	5
x.x.x.x	0	0	0	0
x.x.x.x	0	0	0	0
x.x.x.x	0	0	0	0
x.x.x.x	0	0	0	0
x.x.x.x	0	0	0	0
x.x.x.x	8	114	26	5
x.x.x.x	0	0	0	0
x.x.x.x	9	148	36	5
x.x.x.x	9	141	36	5
x.x.x.x	0	0	10	0
x.x.x.x	3	136	41	6
x.x.x.x	0	0	8	1
x.x.x.x	0	0	0	0
x.x.x.x	5	143	42	6
x.x.x.x	0	0	0	0
x.x.x.x	31	138	31	2
x.x.x.x	3	138	41	6
x.x.x.x	4	139	42	6
x.x.x.x	7	144	42	6
x.x.x.x	0	0	0	0
x.x.x.x	0	0	30	3
x.x.x.x	0	0	14	3
x.x.x.x	0	0	3	0

Report Generated on: 4/3/2017 5:06 PM
Services provided by: Innovative Computer Systems

Vulnerability Assessment & Compliance Report

IP	Critical	High	Medium	Low
x.x.x.x	0	1	8	1
x.x.x.x	0	0	0	0
x.x.x.x	0	0	0	0
x.x.x.x	0	0	0	0
x.x.x.x	0	0	8	1
x.x.x.x	0	0	0	0
x.x.x.x	0	0	3	1
x.x.x.x	0	0	0	0
x.x.x.x	0	0	4	0
x.x.x.x	0	0	0	0
x.x.x.x	0	0	0	0
x.x.x.x	0	0	0	0
x.x.x.x	7	189	61	10
x.x.x.x	0	0	1	0
x.x.x.x	0	0	9	0

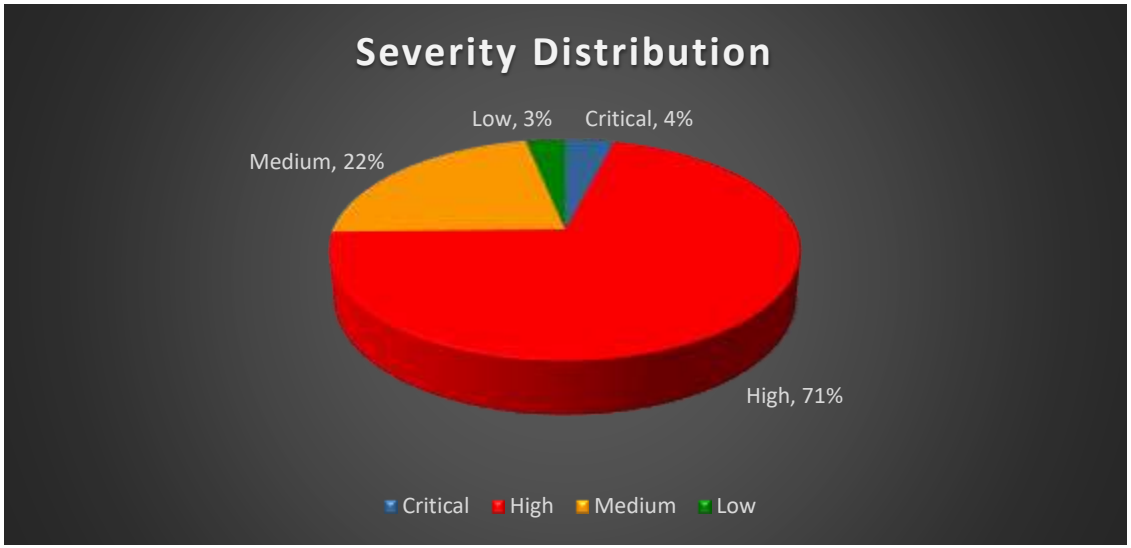
Report Generated on: 4/3/2017 5:06 PM
Services provided by: Innovative Computer Systems

Vulnerability Assessment & Compliance Report

2.2.2 Total Amount of Vulnerabilities per Category

The table & pie chart below presents an overall view of the number of potential vulnerabilities that exist in each category.

Critical	High	Medium	Low
131	2283	717	104



2.2.3 Vulnerabilities and Affected Devices

All vulnerabilities identified by Nessus with a severity of *Medium* or higher, are presented below. Information about each vulnerability is presented together with the affected devices. The vulnerabilities are sorted by severity, with the most severe vulnerabilities first.

Synopsis	The remote host is affected by multiple elevation of privilege vulnerabilities.
Severity	Critical
Risk	Critical
Solution	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, RT 8.1, 2012 R2, and 10. Note that cumulative update 3160005 in MS16-063 must also be installed in order to fully resolve CVE-2016-3213.
CVE numbers	CVE-2016-3213 CVE-2016-3236 CVE-2016-3299

Vulnerability Assessment & Compliance Report

Affected IP addresses	x.x.x..154 x.x.x..153 x.x.x..150 x.x.x..148 x.x.x..143 x.x.x..139 x.x.x..138 x.x.x..134 x.x.x..126 x.x.x..125 x.x.x..120 x.x.x..118 x.x.x..117 x.x.x..6

Synopsis	**The remote Windows host is affected by a vulnerability in the HTTP protocol stack.**
Severity	Critical
Risk	Critical
Solution	Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 8.1, 2012, and 2012 R2
CVE numbers	CVE-2015-1635
Affected IP addresses	x.x.x..154 x.x.x..153 x.x.x..150 x.x.x..148 x.x.x..143 x.x.x..139 x.x.x..138 x.x.x..120 x.x.x..118 x.x.x..117 x.x.x..6

Vulnerability Assessment & Compliance Report

Synopsis	The remote host contains an unsupported Channel version of Microsoft Office 365.
Severity	Critical
Risk	Critical
Solution	Upgrade to a Channel version of Microsoft Office 365 that is currently supported.
CVE numbers	
Affected IP addresses	x.x.x..154 x.x.x..138 x.x.x..134 x.x.x..126 x.x.x..120 x.x.x..118 x.x.x..117

Synopsis	The remote Windows host is affected by multiple vulnerabilities.
Severity	High
Risk	High
Solution	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2. Additionally, Microsoft has released a set of patches for Office 2007, Office 2010, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013, Lync Basic 2013; and .NET Framework 3.0, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2.
CVE numbers	CVE-2015-1670 CVE-2015-1671
Affected IP addresses	x.x.x..154 x.x.x..153 x.x.x..150 x.x.x..148 x.x.x..143 x.x.x..139 x.x.x..138 x.x.x..120 x.x.x..118 x.x.x..117 x.x.x..106 x.x.x..6

Vulnerability Assessment & Compliance Report

Synopsis	The remote Windows host has an antimalware application that is affected by a privilege escalation vulnerability.
Severity	High
Risk	High
Solution	Enable automatic updates to update the scan engine for the relevant antimalware applications. Refer to KB2510781 for information on how to verify MMPE (and the associated MSRT) has been updated.
CVE numbers	CVE-2015-2418
Affected IP addresses	x.x.x..154 x.x.x..153 x.x.x..150 x.x.x..148 x.x.x..143 x.x.x..139 x.x.x..138 x.x.x..125 x.x.x..120 x.x.x..118 x.x.x..117

Synopsis	The version of Adobe Reader installed on the remote Windows host is affected by multiple vulnerabilities.
Severity	High
Risk	High
Solution	Upgrade to Adobe Reader version 11.0.17 / 15.006.30198 / 15.017.20050 or later.

Vulnerability Assessment & Compliance Report

CVE numbers	CVE-2016-4191
	CVE-2016-4192
	CVE-2016-4193
	CVE-2016-4194
	CVE-2016-4195
	CVE-2016-4196
	CVE-2016-4197
	CVE-2016-4198
	CVE-2016-4199
	CVE-2016-4200
	CVE-2016-4201
	CVE-2016-4202
	CVE-2016-4203
	CVE-2016-4204
	CVE-2016-4205
	CVE-2016-4206
	CVE-2016-4207
	CVE-2016-4208
	CVE-2016-4209
	CVE-2016-4210
	CVE-2016-4211
	CVE-2016-4212
	CVE-2016-4213
	CVE-2016-4214
	CVE-2016-4215
	CVE-2016-4250
	CVE-2016-4251
	CVE-2016-4252
	CVE-2016-4254
	CVE-2016-4255
	CVE-2016-4265
	CVE-2016-4266
	CVE-2016-4267
	CVE-2016-4268
	CVE-2016-4269
	CVE-2016-4270

Vulnerability Assessment & Compliance Report

	CVE-2016-6937 CVE-2016-6938
Affected IP addresses	x.x.x..126
Severity	Medium
Risk	Medium
Solution	Upgrade to Google Chrome 43.0.2357.130 or later.
CVE numbers	CVE-2015-1266 CVE-2015-1267 CVE-2015-1268 CVE-2015-1269
Affected IP addresses	x.x.x..15
Severity	Medium
Risk	Medium
Solution	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, 2008 R2, 8, and 2012.
CVE numbers	CVE-2013-1282
Affected IP addresses	x.x.x..6

Synopsis	**The version of Symantec Endpoint Protection Manager installed on the remote host is affected by multiple vulnerabilities.**
Severity	Medium
Risk	Medium
Solution	Upgrade to Symantec Endpoint Protection Manager 12.1 RU6 or later.
CVE numbers	CVE-2014-9227 CVE-2014-9228 CVE-2014-9229
Affected IP addresses	x.x.x..6

3 Compliance Results

3.1 HIPAA Compliance

3.1.1 Overview

This section provides an overview of HIPAA compliance within the organization. Each device is tested with certain compliance rules and values that determine if the device passes or fails compliance.

Check name	Result
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Application Log Restrict Guest Access'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum Application Log Size (KB)'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum Security Log Size (KB)'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum System Log Size (KB)'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain application log'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain security log'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain system log'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Security Log Restrict Guest Access'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'System Log Restrict Guest Access'	PASSED
HIPAA 164.308(a)(5)(ii)(B) - Protection from Malicious Software	PASSED
HIPAA 164.308(a)(5)(ii)(B) - Protection from Malicious Software	FAILED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_ACCOUNT_LOGON'	PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_ACCOUNT_MANAGER'	PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_LOGON'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Account Lockout Duration	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Account Lockout Threshold	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Account Logon Events	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Account Management	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Logon Events	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Enforce Password History	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Enforce Password History	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Maximum Password Age	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Minimum Password Age	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Minimum Password Age	PASSED

Check name	Result
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Minimum Password Length	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Minimum Password Length	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Password Must Meet Complexity Requirements	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Password Must Meet Complexity Requirements	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Reset Account Lockout Counter After	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Store Passwords Using Reversible Encryption	PASSED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'AutoDisconnect'.	PASSED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'FORCE_LOGOFF'	FAILED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'MaxIdleTime'.	FAILED
HIPAA 164.312(a)(2)(iv) - Encryption and Decryption (A)--Network Servers	PASSED
HIPAA 164.312(a)(2)(iv) - Encryption and Decryption (A)--Symantec or BitLocker	PASSED
HIPAA 164.312(a)(2)(iv) - Encryption and Decryption (A)--Symantec or BitLocker	FAILED
HIPAA 164.312(e)(1) - Transmission Security 'MSFtpsvc'	PASSED
HIPAA 164.312(e)(1) - Transmission Security 'MSFtpsvc'	FAILED
HIPAA 164.312(e)(1) - Transmission Security 'TFTPD'	PASSED
HIPAA 164.312(e)(1) - Transmission Security 'Telnet'	PASSED

3.1.2 Detailed Compliance

This section breaks down on each HIPAA compliance rule and determines if the computer “Passed” or “Failed” compliance.

3.1.2.1 Device IP: x.x.x.139

Operating system: Microsoft Windows 7 Professional Service Pack 1

Computer Name: FD4

Check name	Policy Value	Actual Value	Result
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Application Log Restrict Guest Access'	'enabled'	'enabled'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum Application Log Size (KB)'	[32768..4294967295]	NULL	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum Security Log Size (KB)'	[81920..4294967295]	NULL	PASSED

Vulnerability Assessment & Compliance Report

Check name	Policy Value	Actual Value	Result
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum System Log Size (KB)'	[32768..4294967295]	NULL	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain application log'	[365..4294967295]	365	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain security log'	[365..4294967295]	365	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain system log'	[365..4294967295]	365	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Security Log Restrict Guest Access'	'enabled'	'enabled'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'System Log Restrict Guest Access'	'enabled'	'enabled'	PASSED
HIPAA 164.308(a)(5)(ii)(B) - Protection from Malicious Software			PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_ACCOUNT_LOGON'	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_ACCOUNT_MANAGER'	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_LOGON'	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Account Lockout Duration	[0..4294967295]	30	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Account Lockout Threshold	[0..6]	0	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Account Logon Events	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Account Management	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Logon Events	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Enforce Password History	[4..4294967295]	0	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Maximum Password Age	[0..180]	0	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Minimum Password Age	[1..4294967295]	0	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Minimum Password Length	[7..4294967295]	0	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Password Must Meet Complexity Requirements	'enabled'	'disabled'	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Reset Account Lockout Counter After	[6..4294967295]	30	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Store Passwords Using Reversible Encryption	'disabled'	'disabled'	PASSED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'AutoDisconnect'.	[1..15]	15	PASSED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'FORCE_LOGOFF'	'enabled'	'disabled'	FAILED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'MaxIdleTime'.	[0..28000000]	NULL	FAILED
HIPAA 164.312(a)(2)(iv) - Encryption and Decryption (A)--Symantec or BitLocker			PASSED

Check name	Policy Value	Actual Value	Result
HIPAA 164.312(e)(1) - Transmission Security 'MSFtpsvc'	'disabled'	NULL	PASSED
HIPAA 164.312(e)(1) - Transmission Security 'TFTPD'	'disabled'	NULL	PASSED
HIPAA 164.312(e)(1) - Transmission Security 'Telnet'	'disabled'	NULL	PASSED

3.1.2.2 Device IP: x.x.x..143

Operating system: Microsoft Windows 7 Professional Service Pack 1

Computer Name: CL

Check name	Policy Value	Actual Value	Result
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Application Log Restrict Guest Access'	'enabled'	'enabled'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum Application Log Size (KB)'	[32768..4294967295]	NULL	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum Security Log Size (KB)'	[81920..4294967295]	NULL	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum System Log Size (KB)'	[32768..4294967295]	NULL	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain application log'	[365..4294967295]	365	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain security log'	[365..4294967295]	365	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain system log'	[365..4294967295]	365	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Security Log Restrict Guest Access'	'enabled'	'enabled'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'System Log Restrict Guest Access'	'enabled'	'enabled'	PASSED
HIPAA 164.308(a)(5)(ii)(B) - Protection from Malicious Software			PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_ACCOUNT_LOGON'	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_ACCOUNT_MANAGER'	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_LOGON'	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Account Lockout Duration	[0..4294967295]	30	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Account Lockout Threshold	[0..6]	0	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Account Logon Events	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Account Management	'success, failure'	'success, failure'	PASSED

Check name	Policy Value	Actual Value	Result
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Logon Events	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Enforce Password History	[4..4294967295]	0	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Maximum Password Age	[0..180]	0	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Minimum Password Age	[1..4294967295]	0	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Minimum Password Length	[7..4294967295]	0	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Password Must Meet Complexity Requirements	'enabled'	'disabled'	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Reset Account Lockout Counter After	[6..4294967295]	30	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Store Passwords Using Reversible Encryption	'disabled'	'disabled'	PASSED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'AutoDisconnect'.	[1..15]	15	PASSED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'FORCE_LOGOFF'	'enabled'	'disabled'	FAILED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'MaxIdleTime'.	[0..28000000]	NULL	FAILED
HIPAA 164.312(a)(2)(iv) - Encryption and Decryption (A)--Symantec or BitLocker			PASSED
HIPAA 164.312(e)(1) - Transmission Security 'MSFtpsvc'	'disabled'	NULL	PASSED
HIPAA 164.312(e)(1) - Transmission Security 'TFTPD'	'disabled'	NULL	PASSED
HIPAA 164.312(e)(1) - Transmission Security 'Telnet'	'disabled'	NULL	PASSED

3.1.2.3 Device IP: x.x.x..148

Operating system: Microsoft Windows 7 Professional Service Pack 1

Computer Name: FD1

Check name	Policy Value	Actual Value	Result
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Application Log Restrict Guest Access'	'enabled'	'enabled'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum Application Log Size (KB)'	[32768..4294967295]	NULL	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum Security Log Size (KB)'	[81920..4294967295]	NULL	PASSED

Vulnerability Assessment & Compliance Report

Check name	Policy Value	Actual Value	Result
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Maximum System Log Size (KB)'	[32768..4294967295]	NULL	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain application log'	[365..4294967295]	365	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain security log'	[365..4294967295]	365	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Retain system log'	[365..4294967295]	365	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'Security Log Restrict Guest Access'	'enabled'	'enabled'	PASSED
HIPAA 164.308(a)(1)(ii)(D) - Information System Activity Review (R) 'System Log Restrict Guest Access'	'enabled'	'enabled'	PASSED
HIPAA 164.308(a)(5)(ii)(B) - Protection from Malicious Software			PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_ACCOUNT_LOGON'	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_ACCOUNT_MANAGER'	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(C) - Log-in Monitoring (A) 'AUDIT_LOGON'	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Account Lockout Duration	[0..4294967295]	30	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Account Lockout Threshold	[0..6]	0	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Account Logon Events	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Account Management	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Audit Logon Events	'success, failure'	'success, failure'	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Enforce Password History	[4..4294967295]	0	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Maximum Password Age	[0..180]	0	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Minimum Password Age	[1..4294967295]	0	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Minimum Password Length	[7..4294967295]	0	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Password Must Meet Complexity Requirements	'enabled'	'disabled'	FAILED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Reset Account Lockout Counter After	[6..4294967295]	30	PASSED
HIPAA 164.308(a)(5)(ii)(D) - Password Management (A) - Store Passwords Using Reversible Encryption	'disabled'	'disabled'	PASSED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'AutoDisconnect'.	[1..15]	15	PASSED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'FORCE_LOGOFF'	'enabled'	'disabled'	FAILED
HIPAA 164.312(a)(2)(iii) - Automatic Logoff (A): Terminate an electronic session after a predetermined time of inactivity 'MaxIdleTime'.	[0..28000000]	NULL	FAILED
HIPAA 164.312(a)(2)(iv) - Encryption and Decryption (A)--Symantec or BitLocker			PASSED

Check name	Policy Value	Actual Value	Result
HIPAA 164.312(e)(1) - Transmission Security 'MSFtpsvc'	'disabled'	NULL	PASSED
HIPAA 164.312(e)(1) - Transmission Security 'TFTPD'	'disabled'	NULL	PASSED
HIPAA 164.312(e)(1) - Transmission Security 'Telnet'	'disabled'	NULL	PASSED

4 Remediation Results

4.1 Findings

The section provides an overview of the corrective action that should take place to minimize the vulnerabilities found in this report.

Description	Remediation	Severity	Count
Symantec Antivirus Software Detection and Status	Ensure that updates are working and the associated services are running.	Critical	2
Microsoft .NET Framework Service Pack Out of Date	Install the latest Microsoft .NET Framework service pack.	Critical	1
MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	Microsoft has released a set of patches for .NET Framework 2.0 SP2, 3.5, 3.5.1, 4.0, 4.5, 4.5.1, and 4.5.2.	Critical	2
MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (remote check)	Microsoft has released a set of patches for Windows 2003, 2008, and 2008 R2.	Critical	2
MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)	Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 8.1, 2012, and 2012 R2	Critical	11
MS15-067: Vulnerability in RDP Could Allow Remote Code Execution (3073094)	Microsoft has released a set of patches for Windows 7, 8, and 2012.	Critical	11
MS16-077: Security Update for WPAD (3165191)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, RT 8.1, 2012 R2, and 10. Note that cumulative update 3160005 in MS16-063 must also be installed in order to fully resolve CVE-2016-3213.	Critical	14
Oracle Java SE Multiple Vulnerabilities (April 2013 CPU)	Update to JDK / JRE 5 Update 45, 6 Update 45, 7 Update 21 or later and, if necessary, remove any affected versions. Note that an Extended Support contract with Oracle is needed to obtain JDK / JRE 5 Update 45 or later.	Critical	1

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
Oracle Java SE Multiple Vulnerabilities (June 2013 CPU)	Update to JDK / JRE 5 Update 51, 6 Update 51, 7 Update 25 or later and, if necessary, remove any affected versions. Note that an Extended Support contract with Oracle is needed to obtain JDK / JRE 5 Update 51 or later or 6 Update 51 or later.	Critical	1
Oracle Java JDK / JRE 6 < Update 20 Multiple Vulnerabilities	Update to JDK / JRE 6 Update 20 or later and remove if necessary any affected versions.	Critical	1
Oracle Java SE Multiple Vulnerabilities (October 2010 CPU)	Update to JDK / JRE 6 Update 22, JDK 5.0 Update 26, SDK 1.4.2_28 or later and remove if necessary any affected versions. Note that an Extended Support contract with Oracle is needed to obtain JDK 5.0 Update 26 or later.	Critical	1
Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Update to JDK / JRE 6 Update 24, JDK 5.0 Update 28, SDK 1.4.2_30 or later and remove if necessary any affected versions. Note that an Extended Support contract with Oracle is needed to obtain JDK 5.0 Update 28 or later.	Critical	1
Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	Update to JDK / JRE 6 Update 26, JDK 5.0 Update 30, SDK 1.4.2_32 or later and remove, if necessary, any affected versions. Note that an Extended Support contract with Oracle is needed to obtain JDK 5.0 Update 30 or later.	Critical	1
Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Update to JDK / JRE 6 Update 30 or later and remove, if necessary, any affected versions.	Critical	1
Oracle Java JDK / JRE 6 < Update 35 SunToolKit getField() and getMethod() Access Issue	Update to JDK / JRE 6 Update 35 or later and remove, if necessary, any affected versions.	Critical	1
Oracle Java SE Multiple Vulnerabilities (October 2011 CPU) (BEAST)	Update to JDK / JRE 7 Update 1 / 6 Update 29, JDK 5.0 Update 32, SDK 1.4.2_34 or later and remove, if necessary, any affected versions. Note that an Extended Support contract with Oracle is needed to obtain JDK 5.0 Update 32 or later.	Critical	1
MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)	Microsoft has released a set of patches for .NET Framework 1.0, 1.1, 2.0, 3.0, 3.5, and 4.	High	1
MS12-025: Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)	Microsoft has released a set of patches for .NET Framework 1.0, 1.1, 2.0, 3.5.1, and 4.	High	1
MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3057134)	Microsoft has released a set of patches for .NET Framework 1.1 SP1, 2.0 SP2, 3.5, 3.5.1, 4.0, 4.5, 4.5.1, and 4.5.2.	High	13
MS14-009: Vulnerabilities in .NET Framework Could Allow Privilege Escalation (2916607)	Microsoft has released a set of patches for .NET Framework 1.1 SP1, 2.0 SP2, 3.5, 3.5.1, 4.0, 4.5, and 4.5.1.	High	2
MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2878890)	Microsoft has released a set of patches for .NET Framework 2.0, 3.0, 3.5, 3.5.1, 4.0, and 4.5.	High	2

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3089662)	Microsoft has released a set of patches for .NET Framework 2.0, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6.	High	14
MS12-038: Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)	Microsoft has released a set of patches for .NET Framework 2.0, 3.5, and 4.	High	1
MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842)	Microsoft has released a set of patches for .NET Framework 2.0, 3.5, and Silverlight.	High	1
MS12-016: Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)	Microsoft has released a set of patches for .NET Framework 2.0, 3.5.1, and 4 as well as Silverlight 4.	High	1
MS16-019: Security Update for .NET Framework to Address Denial of Service (3137893)	Microsoft has released a set of patches for .NET framework 2.0 SP2, 3.5, 3.5.1, 4, 4.5.1, 4.5.2, 4.6, and 4.6.1.	High	14
MS15-021: Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (3032323)	Microsoft has released a set of patches for 2003, Vista, 2008, 7, 2008 R2, 8, Windows RT, 2012, 8.1, Windows RT 8.1, and 2012 R2.	High	11
MS09-021: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)	Microsoft has released a set of patches for Excel 2000, 2002, 2003, and 2007, Excel Viewer and Excel Viewer 2003 as well as the 2007 Microsoft Office system and the Microsoft Office Compatibility Pack.	High	2
MS08-043: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (954066)	Microsoft has released a set of patches for Excel 2000, XP, 2003 and 2007.	High	2
MS15-009: Security Update for Internet Explorer (3034682)	Microsoft has released a set of patches for Internet Explorer 6, 7, 8, 9, 10, and 11.	High	68
MS15-079: Cumulative Security Update for Internet Explorer (3082442)	Microsoft has released a set of patches for Internet Explorer 7, 8, 9, 10, and 11.	High	28
MS16-142: Cumulative Security Update for Internet Explorer (3198467)	Microsoft has released a set of patches for Internet Explorer 9, 10, and 11.	High	75
MS16-104: Cumulative Security Update for Internet Explorer (3183038)	Microsoft has released a set of patches for Internet Explorer 9, 10, and 11. Note that MS16-116 must also be installed to fully resolve CVE-2016-3375.	High	15
MS16-118: Cumulative Security Update for Internet Explorer (3192887)	Microsoft has released a set of patches for Internet Explorer 9, 10, and 11. Note that security update 3193515 in MS16-126 must also be installed in order to fully resolve CVE-2016-3298 on Windows Vista and Windows Server 2008.	High	15

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
MS16-144: Cumulative Security Update for Internet Explorer (3204059)	Microsoft has released a set of patches for Internet Explorer 9, 10, and 11. Note that security update 3208481 in MS16-144 must also be installed in order to fully resolve CVE-2016-7278 on Windows Vista and Windows Server 2008.	High	15
MS16-063: Cumulative Security Update for Internet Explorer (3163649)	Microsoft has released a set of patches for Internet Explorer 9, 10, and 11. Note that the security update in MS16-077 must also be installed in order to fully resolve CVE-2016-3213.	High	15
MS12-060: Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2720573)	Microsoft has released a set of patches for Microsoft Office 2003, 2007, and 2010, Office 2003 Web Components, Microsoft SQL Server 2000, Microsoft SQL Analysis Services 2000, Microsoft Commerce Server 2002, 2007, and 2009, Microsoft Host Integration Server 2004, Microsoft Visual Fox Pro 8.0 and 9.0, and Visual Basic 6.0 Runtime.	High	1
MS16-107: Security Update for Microsoft Office (3185852)	Microsoft has released a set of patches for Microsoft Office 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Excel 2007, 2010, 2013, 2013 RT, and 2016; Microsoft PowerPoint 2007, 2010, 2013, and 2013 RT; Microsoft Outlook 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Visio 2016; Office Compatibility Pack; Excel Viewer; PowerPoint Viewer; Word Viewer; Microsoft SharePoint Server 2007, 2010, and 2013; Office Web Apps 2010 and 2013; and Office Online Server.	High	1
MS16-133: Security Update for Microsoft Office (3199168)	Microsoft has released a set of patches for Microsoft Office 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Excel 2007, 2010, 2013, 2013 RT, and 2016; Microsoft PowerPoint 2010; Microsoft Word 2007, 2010, 2013, and 2013 RT; Office Compatibility Pack; Excel Viewer; PowerPoint Viewer; Word Viewer; Microsoft SharePoint Server 2010 and 2013; and Office Web Apps 2010 and 2013	High	7
MS16-148: Security Update for Microsoft Office (3204068)	Microsoft has released a set of patches for Microsoft Office 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Excel 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Word 2007, 2010; Microsoft Publisher 2010 Office Compatibility Pack; Excel Viewer; Word Viewer; Microsoft SharePoint Server 2007 and 2010; and Office Web Apps 2010.	High	7

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
MS16-070: Security Update for Microsoft Office (3163610)	Microsoft has released a set of patches for Microsoft Office 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Word 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Excel 2007 and 2010; Microsoft Visio 2007, 2010, 2013, and 2016; Visio Viewer 2007 and 2010; Word Viewer; Microsoft Office Compatibility Pack; Office Web Apps 2010 and 2013; Microsoft SharePoint Server 2010 and 2013; and Office Online Server.	High	1
MS16-088: Security Update for Microsoft Office (3170008)	Microsoft has released a set of patches for Microsoft Office 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Word 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Excel 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Outlook 2010, 2013, 2013 RT, and 2016; Microsoft PowerPoint 2010, 2013, and 2013 RT; Excel Viewer; Word Viewer; Microsoft Office Compatibility Pack; Office Web Apps 2010 and 2013; Microsoft SharePoint Server 2010, 2013 and 2016; Microsoft SharePoint Foundation 2010 and 2013; and Office Online Server.	High	1
MS16-121: Security Update for Microsoft Office (3194063)	Microsoft has released a set of patches for Microsoft Office 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Word 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Office Compatibility Pack; Microsoft Word Viewer; Microsoft SharePoint Server 2010 and 2013; Microsoft Office Web Apps 2010 and 2013; and Office Online Server.	High	1
MS16-099: Security Update for Microsoft Office (3177451)	Microsoft has released a set of patches for Microsoft Office 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Word 2007, 2010, 2013, 2013 RT, and 2016; Microsoft OneNote 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Outlook 2007, 2010, 2013, and 2016; and Word Viewer.	High	1
MS16-054: Security Update for Microsoft Office (3155544)	Microsoft has released a set of patches for Microsoft Office 2007, 2010, 2013, 2013 RT, and 2016; Microsoft Word 2007, 2010, 2013, 2013 RT, and 2016; Word Viewer; Microsoft Office Compatibility Pack; Office Web Apps 2010; and Microsoft SharePoint Server 2010.	High	1
MS16-042: Security Update for Microsoft Office (3148775)	Microsoft has released a set of patches for Microsoft Office 2010; Microsoft Word 2007, 2010, 2013, and 2013 RT; Microsoft Excel 2007, 2010, 2013, 2013 RT, and 2016; Word Viewer; Excel Viewer; SharePoint Server 2007, 2010, and 2013; Microsoft Office Compatibility Pack; and Office Web Apps 2010 and 2013.	High	1

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
MS10-038: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Microsoft has released a set of patches for Office Excel 2002, Office Excel 2003, Excel 2007, Office Excel Viewer and Office Compatibility Pack.	High	2
MS11-021: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2489279)	Microsoft has released a set of patches for Office XP, 2003, 2007, 2010, Excel Viewer, and Office Compatability Pack.	High	2
MS10-080: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Microsoft has released a set of patches for Office XP, 2003, 2007, and Excel Viewer.	High	1
MS16-109: Security Update for Silverlight (3182373)	Microsoft has released a set of patches for Silverlight 5.	High	5
MS16-116: Security Update in OLE Automation for VBScript Scripting Engine (3188724)	Microsoft has released a set of patches for Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10	High	16
MS16-034: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3143145)	Microsoft has released a set of patches for Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.	High	14
MS15-094: Cumulative Security Update for Internet Explorer (3089548)	Microsoft has released a set of patches for Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, 2012 R2, and 10.	High	40
MS15-133: Security Update for Windows PGM to Address Elevation of Privilege (3116130)	Microsoft has released a set of patches for Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10.	High	14
MS15-114: Security Update for Windows Journal to Address Remote Code Execution (3100213)	Microsoft has released a set of patches for Vista, 2008, 7, and 2008 R2.	High	13
MS15-134: Security Update for Windows Media Center to Address Remote Code Execution (3108669)	Microsoft has released a set of patches for Vista, 7, 8, and 8.1.	High	13
MS11-025: Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212)	Microsoft has released a set of patches for Visual Studio .NET 2003, 2005, and 2008, as well as Visual C++ 2005, 2008, and 2010.	High	4
MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (955218)	Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, 2008, 7, and 2008 R2.	High	5
MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191)	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.	High	89

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
MS15-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (3038680)	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2. KB3035131 (MS15-025) has affected binaries in common with Security Advisory 3033929, which was released simultaneously. If you download and install updates manually, you should first install KB3035131 (MS15-025) before installing KB3033929. See the MS15-025 bulletin Update FAQ for more information.	High	11
MS15-044: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (3057110)	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2. Additionally, Microsoft has released a set of patches for Office 2007, Office 2010, Live Meeting 2007 Console, Lync 2010, Lync 2010 Attendee, Lync 2013, Lync Basic 2013; and .NET Framework 3.0, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2.	High	12
MS15-077: Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (3077657)	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, and 2012 R2.	High	22
MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution (3072631)	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8.1, and 2012 R2.	High	11
MS15-035: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3046306)	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, and 2008 R2.	High	21
MS16-076: Security Update for Netlogon (3167691)	Microsoft has released a set of patches for Windows 2008, 2008 R2, 2012, and 2012 R2.	High	2
MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (3023266)	Microsoft has released a set of patches for Windows 2008, 7, 2008 R2, 8, 8.1, 2012 and 2012 R2.	High	10
MS17-005: Security Update for Adobe Flash Player (4010250)	Microsoft has released a set of patches for Windows 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016.	High	1
MS15-130: Security Update for Microsoft Uniscribe to Address Remote Code Execution (3108670)	Microsoft has released a set of patches for Windows 7 and 2008 R2.	High	14
MS16-027: Security Update for Windows Media to Address Remote Code Execution (3143146)	Microsoft has released a set of patches for Windows 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.	High	13
MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass (3030377)	Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.	High	22

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution (2912390)	Microsoft has released a set of patches for Windows 7, 2008, 8, 8.1, 2012 and 2012 R2.	High	2
MS16-017: Security Update for Remote Desktop Display Driver to Address Elevation of Privilege (3134700)	Microsoft has released a set of patches for Windows 7, 2012, 8.1, 2012 R2, and 10.	High	13
MS16-112: Security Update for Windows Lock Screen (3178469)	Microsoft has released a set of patches for Windows 8.1, RT 8.1, 2012 R2, and 10.	High	1
MS16-030: Security Update for Windows OLE to Address Remote Code Execution (3143136)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, 2012 R2, and 10.	High	41
MS16-149: Security Update for Microsoft Windows (3205655)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016.	High	135
MS16-023: Cumulative Security Update for Internet Explorer (3142015)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.	High	345
MS16-120: Security Update for Microsoft Graphics Component (3192884)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. Additionally, Microsoft has released a set of patches for Office 2007, Office 2010, Word Viewer, Skype for Business 2016, Lync 2010, Lync 2013, Live Meeting 2007 Console, .NET Framework 3.0 SP2, .NET Framework 3.5, .NET Framework 3.5.1, .NET Framework 4.5.2, .NET Framework 4.6, and Silverlight 5.	High	15
MS16-039: Security Update for Microsoft Graphics Component (3148522)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. Additionally, Microsoft has released a set of patches for Office 2007, Office 2010, Word Viewer, Skype for Business 2016, Lync 2010, Lync 2013, Live Meeting 2007 Console, .NET framework 3.0 SP2, .NET framework 3.5, and .NET framework 3.5.1.	High	15
MS16-044: Security Update for Windows OLE (3146706)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, and 2012 R2.	High	14
MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (3089657)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, 2012 R2, 10.	High	13
MS15-109: Security Update for Windows Shell to Address Remote Code Execution (3096443)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, 2012 R2, and 10.	High	27
MS15-045: Vulnerability in Windows Journal Could Allow Remote Code Execution (3046002)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2	High	10

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.	High	43
MS15-112: Cumulative Security Update for Internet Explorer (3104517)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10.	High	145
MS16-005: Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution (3124584)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10. Note that Windows 10 with Citrix XenDesktop installed will not be offered the patch due to an issue with the XenDesktop software that prevents users from logging on when the patch is applied. To apply the patch you must first uninstall XenDesktop or contact Citrix for help with the issue.	High	58
MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10. Additionally, Microsoft has released a set of patches for Office 2007, Office 2010, Lync 2010, Lync 2010 Attendee, Lync 2013 (Skype for Business), Lync Basic 2013, and Live Meeting 2007.	High	13
MS15-080 : Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10. Additionally, Microsoft has released a set of patches for Office 2007, Office 2010, Microsoft Lync 2010, 2010 Attendee, 2013 SP1, Microsoft Live Meeting 2007; and .NET Framework 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6.	High	14
MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10. Additionally, Microsoft has released a set of patches for Office 2007, Office 2010, Word Viewer, Lync 2010, Lync 2010 Attendee, Lync 2013, Lync Basic 2013, Skype for Business 2016, Live Meeting 2007 Console, Silverlight; and .NET framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5.1, 4.5.2, and 4.6.	High	15
MS15-063: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (3063858)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, and 2012.	High	11
MS16-060: Security Update for Windows Kernel (3154846)	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10.	High	14
MS16-031: Security Update for Microsoft Windows to Address Elevation of Privilege (3140410)	Microsoft has released a set of patches for Windows Vista, 2008, 7, and 2008 R2	High	14

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
MS17-004: Security Update for Local Security Authority Subsystem Service (3216771)	Microsoft has released a set of patches for Windows Vista, 2008, 7, and 2008 R2.	High	29
MS15-100: Vulnerability in Windows Media Center Could Allow Remote Code Execution (3087918)	Microsoft has released a set of patches for Windows Vista, 7, 8, and 8.1.	High	12
MS16-122: Security Update for Microsoft Video Control (3195360)	Microsoft has released a set of patches for Windows Vista, 7, 8.1, RT 8.1, and 10.	High	26
MS16-056: Security Update for Windows Journal (3156761)	Microsoft has released a set of patches for Windows Vista, 7, 8.1, RT 8.1, and 10. Alternatively, apply the workaround referenced in the vendor advisory.	High	13
MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, 2008 R2; Office 2003, 2007, and 2010; .NET Framework 3.0, 3.5.1, and 4.0; and Silverlight 4 and 5.	High	14
MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://support.microsoft.com/kb/2264107 Please note this update provides a method of mitigating a class of vulnerabilities rather than fixing any specific vulnerabilities. Additionally, these patches must be used in conjunction with the 'CWDIllegalInDllSearch' registry setting to have any effect. These protections could be applied in a way that breaks functionality in existing applications. Refer to the Microsoft advisory for more information.	High	19
MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2, 8, 2012, Office 2003, 2007, Word Viewer, Office Compatibility Pack, Expression Web Service, Expression Web 2, SharePoint Server 2007 and Groove Server 2007.	High	1
MS11-095: Vulnerability in Active Directory Could Allow Remote Code Execution (2640045)	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.	High	2
MS13-054: Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)	Microsoft has released a set of patches for Windows, Office 2003, Office 2007, Office 2010, Lync 2010, Lync 2010 Attendee, Lync 2013, and Lync Basic 2013.	High	3
MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service (2769327)	Microsoft has released a set of patches for the .NET Framework on Windows XP, 2003, Vista, 2008, 7, 2008 R2, 8, and 2012.	High	5
MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814)	Microsoft has released a set of patches for the .NET Framework on Windows XP, 2003, Vista, 2008, 7, and 2008 R2.	High	5

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
MS KB2506014: Update for the Windows Operating System Loader	Microsoft has released a set of patches for the 64-bit editions of Windows Vista, 2008, 7, and 2008 R2 : http://support.microsoft.com/kb/2506014	High	1
Microsoft Windows Update Reboot Required	Reboot the remote system to put pending changes into effect.	High	3
IPMI v2.0 Password Hash Disclosure	There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include : - Disabling IPMI over LAN if it is not needed. - Using strong passwords to limit the successfulness of off-line dictionary attacks. - Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.	High	2
Oracle Java SE Multiple Vulnerabilities (March 2010 CPU)	Update to JDK / JRE 6 Update 19, JDK 5.0 Update 24, SDK 1.4.2_26 or later and remove if necessary any affected versions. Note that an Extended Support contract with Oracle is needed to obtain JDK 5.0 Update 24 or later.	High	1
Oracle Java JDK / JRE 6 < Update 43 Remote Code Execution (Windows)	Update to JDK / JRE 6 Update 43 or later and remove, if necessary, any affected versions.	High	1
Sun Java JRE Multiple Vulnerabilities (244986 et al)	Update to Sun Java JDK / JRE 6 Update 11, JDK / JRE 5.0 Update 17, SDK / JRE 1.4.2_19, or SDK / JRE 1.3.1_24 or later and remove if necessary any affected versions.	High	1
Sun Java JRE Multiple Vulnerabilities (254569 / 254611 / 254608 ..)	Update to Sun Java JDK / JRE 6 Update 13, JDK / JRE 5.0 Update 18, SDK / JRE 1.4.2_20, or SDK / JRE 1.3.1_25 or later and remove, if necessary, any affected versions.	High	1
Sun Java JRE Multiple Vulnerabilities (263408 / 263409 / 263428 ..)	Update to Sun Java JDK / JRE 6 Update 15, JDK / JRE 5.0 Update 20, SDK / JRE 1.4.2_22, or SDK / JRE 1.3.1_26 or later and remove, if necessary, any affected versions.	High	1
Sun Java JRE Multiple Vulnerabilities (269868 / 269869 / 270476 ..)	Update to Sun Java JDK / JRE 6 Update 17, JDK / JRE 5.0 Update 22, SDK / JRE 1.4.2_24, or SDK / JRE 1.3.1_27 or later and remove, if necessary, any affected versions.	High	1
Sun Java JDK/JRE 6 < Update 7 Multiple Vulnerabilities	Update to Sun Java JDK and JRE 6 Update 7 or later and remove, if necessary, any affected versions.	High	1
7-Zip < 16.00 Multiple Vulnerabilities	Upgrade to 7-Zip version 16.00 or later.	High	1
Flash Player <= 10.3.183.22 / 11.4.402.264 Multiple Vulnerabilities (APSB12-19)	Upgrade to Adobe Flash Player version 10.3.183.23, 11.4.402.265 or later, or Google Chrome PepperFlash 11.3.31.230 or later.	High	1
Flash Player <= 10.3.183.23 / 11.4.402.278 Multiple Vulnerabilities (APSB12-22)	Upgrade to Adobe Flash Player version 10.3.183.29, 11.4.402.287 or later, or Google Chrome PepperFlash 11.4.31.110 or later.	High	1

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
Flash Player <= 10.3.183.29 / 11.4.402.287 Multiple Vulnerabilities (APSB12-24)	Upgrade to Adobe Flash Player version 10.3.183.43, 11.5.502.110 or later, or Google Chrome PepperFlash 11.5.31.2 or later.	High	1
Flash Player <= 10.3.183.43 / 11.5.502.110 Multiple Vulnerabilities (APSB12-27)	Upgrade to Adobe Flash Player version 10.3.183.48 / 11.5.502.135 or later, or Google Chrome PepperFlash 11.5.31.5 or later.	High	1
Flash Player <= 10.3.183.48 / 11.5.502.135 Buffer Overflow (APSB13-01)	Upgrade to Adobe Flash Player version 10.3.183.50 / 11.5.502.146 or later, or Google Chrome PepperFlash 11.5.31.137 or later.	High	2
Flash Player <= 10.3.183.50 / 11.5.502.146 Multiple Vulnerabilities (APSB13-04)	Upgrade to Adobe Flash Player version 10.3.183.51 / 11.5.502.149 or later, or Google Chrome PepperFlash 11.5.31.139 or later.	High	2
Flash Player <= 10.3.183.51 / 11.5.502.149 Multiple Vulnerabilities (APSB13-05)	Upgrade to Adobe Flash Player version 10.3.183.63 / 11.6.602.168 or later, or Google Chrome PepperFlash 11.6.602.167 or later.	High	2
Flash Player <= 10.3.183.63 / 11.6.602.168 Multiple Vulnerabilities (APSB13-08)	Upgrade to Adobe Flash Player version 10.3.183.67 / 11.6.602.171 or later, or Google Chrome PepperFlash 11.6.602.171 or later.	High	2
Flash Player <= 10.3.183.67 / 11.6.602.171 Multiple Vulnerabilities (APSB13-09)	Upgrade to Adobe Flash Player version 10.3.183.68 / 11.6.602.180 or later, or Google Chrome PepperFlash 11.6.602.180 or later.	High	2
Flash Player <= 10.3.183.68 / 11.6.602.180 Multiple Vulnerabilities (APSB13-11)	Upgrade to Adobe Flash Player version 10.3.183.75 / 11.7.700.169 or later, or Google Chrome PepperFlash 11.7.700.179 or later.	High	2
Flash Player <= 10.3.183.75 / 11.7.700.169 Multiple Vulnerabilities (APSB13-14)	Upgrade to Adobe Flash Player version 10.3.183.86 / 11.7.700.202 or later, or Google Chrome PepperFlash 11.7.700.202 or later.	High	2
Flash Player <= 10.3.183.86 / 11.7.700.202 Memory Corruption (APSB13-16)	Upgrade to Adobe Flash Player version 10.3.183.90 / 11.7.700.224 or later, or Google Chrome PepperFlash 11.7.700.225 or later.	High	2
Flash Player <= 11.3.300.270 Code Execution (APSB12-18)	Upgrade to Adobe Flash Player version 11.3.300.271 later.	High	1
Flash Player <= 10.3.183.90 / 11.7.700.224 Multiple Vulnerabilities (APSB13-17)	Upgrade to Adobe Flash Player version 11.7.700.232 / 11.8.800.94 or later, or Google Chrome PepperFlash 11.8.800.97 or later.	High	2
Flash Player <= 11.7.700.232 / 11.8.800.94 Memory Corruptions (APSB13-21)	Upgrade to Adobe Flash Player version 11.7.700.242 / 11.8.800.168 or later, or Google Chrome Flash 11.8.800.170 or later.	High	2
Flash Player <= 11.7.700.242 / 11.9.900.117 Memory Corruptions (APSB13-26)	Upgrade to Adobe Flash Player version 11.7.700.252 / 11.9.900.152 or later.	High	2
Flash Player <= 11.7.700.252 / 11.9.900.152 Multiple Vulnerabilities (APSB13-28)	Upgrade to Adobe Flash Player version 11.7.700.257 / 11.9.900.170 or later.	High	2
Flash Player <= 11.7.700.257 / 11.9.900.170 Multiple Vulnerabilities (APSB14-02)	Upgrade to Adobe Flash Player version 11.7.700.260 / 12.0.0.38 or later.	High	2
Flash Player <= 11.7.700.260 / 12.0.0.43 Unspecified Remote Code Execution (APSB14-04)	Upgrade to Adobe Flash Player version 11.7.700.261 / 12.0.0.44 or later.	High	2

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
Flash Player <= 11.7.700.261 / 12.0.0.44 Multiple Vulnerabilities (APSB14-07)	Upgrade to Adobe Flash Player version 11.7.700.269 / 12.0.0.70 or later.	High	2
Flash Player <= 11.7.700.272 / 12.0.0.77 Multiple Vulnerabilities (APSB14-09)	Upgrade to Adobe Flash Player version 11.7.700.275 / 13.0.0.182 or later.	High	2
Flash Player <= 11.7.700.275 / 13.0.0.182 Pixel Bender Component Buffer Overflow (APSB14-13)	Upgrade to Adobe Flash Player version 11.7.700.279 / 13.0.0.206 or later.	High	2
Flash Player <= 16.0.0.235 Multiple Vulnerabilities (APSB15-01)	Upgrade to Adobe Flash Player version 16.0.0.257 or later. Alternatively, Adobe has made version 13.0.0.260 available for those installations that cannot be upgraded to 16.x.	High	2
Flash Player <= 16.0.0.287 Unspecified Code Execution (APSA15-01 / APSB15-03)	Upgrade to Adobe Flash Player version 16.0.0.296 or later. Alternatively, Adobe has made version 13.0.0.264 available for those installations that cannot be upgraded to 16.x.	High	2
Flash Player <= 16.0.0.296 Unspecified Code Execution (APSA15-02 / APSB15-04)	Upgrade to Adobe Flash Player version 16.0.0.305 or later. Alternatively, Adobe has made version 13.0.0.269 available for those installations that cannot be upgraded to 16.x.	High	2
Flash Player <= 16.0.0.305 Multiple Vulnerabilities (APSB15-05)	Upgrade to Adobe Flash Player version 17.0.0.134 or later. Alternatively, Adobe has made version 13.0.0.277 available for those installations that cannot be upgraded to 17.x.	High	2
Adobe Flash Player <= 17.0.0.134 Multiple Vulnerabilities (APSB15-06)	Upgrade to Adobe Flash Player version 17.0.0.169 or later. Alternatively, Adobe has made version 13.0.0.281 and 11.2.202.457 available for those installations that cannot be upgraded to 17.x.	High	2
Adobe Flash Player <= 17.0.0.169 Multiple Vulnerabilities (APSB15-09)	Upgrade to Adobe Flash Player version 17.0.0.188 or later. Alternatively, Adobe has made version 13.0.0.289 available for those installations that cannot be upgraded to 17.x.	High	3
Adobe Flash Player <= 17.0.0.188 Multiple Vulnerabilities (APSB15-11)	Upgrade to Adobe Flash Player version 18.0.0.160 or later. Alternatively, Adobe has made version 13.0.0.292 available for those installations that cannot be upgraded to 18.x.	High	3
Adobe Flash Player <= 18.0.0.161 RCE (APSB15-14)	Upgrade to Adobe Flash Player version 18.0.0.194 or later. Alternatively, Adobe has made version 13.0.0.296 available for those installations that cannot be upgraded to 18.x.	High	3
Adobe Flash Player <= 18.0.0.194 Multiple Vulnerabilities (APSB15-16)	Upgrade to Adobe Flash Player version 18.0.0.203 or later. Alternatively, Adobe has made version 13.0.0.302 available for those installations that cannot be upgraded to 18.x.	High	3
Adobe Flash Player <= 18.0.0.203 Multiple RCE Vulnerabilities (APSB15-18)	Upgrade to Adobe Flash Player version 18.0.0.209 or later. Alternatively, Adobe has made version 13.0.0.309 available for those installations that cannot be upgraded to 18.x.	High	3

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
Adobe Flash Player <= 18.0.0.209 Multiple Vulnerabilities (APSB15-19)	Upgrade to Adobe Flash Player version 18.0.0.232 or later.	High	2
Adobe Flash Player <= 18.0.0.232 Multiple Vulnerabilities (APSB15-23)	Upgrade to Adobe Flash Player version 19.0.0.185 or later. Alternatively, Adobe has made version 18.0.0.241 available for those installations that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 19.0.0.185 Multiple Vulnerabilities (APSB15-25)	Upgrade to Adobe Flash Player version 19.0.0.207 or later. Alternatively, Adobe has made version 18.0.0.252 available for those installations that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 19.0.0.207 Vulnerability (APSB15-27)	Upgrade to Adobe Flash Player version 19.0.0.226 or later. Alternatively, Adobe has made version 18.0.0.255 available for those installations that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 19.0.0.226 Multiple Vulnerabilities (APSB15-28)	Upgrade to Adobe Flash Player version 19.0.0.245 or later. Alternatively, Adobe has made version 18.0.0.261 available for those installations that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 19.0.0.245 Multiple Vulnerabilities (APSB15-32)	Upgrade to Adobe Flash Player version 20.0.0.228 or later. Alternatively, Adobe has made version 18.0.0.268 available for those installations that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 20.0.0.235 Multiple Vulnerabilities (APSB16-01)	Upgrade to Adobe Flash Player version 20.0.0.267 or later. Alternatively, Adobe has made version 18.0.0.324 available for those installations that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 20.0.0.286 Multiple Vulnerabilities (APSB16-04)	Upgrade to Adobe Flash Player version 20.0.0.306 or later. Alternatively, Adobe has made version 18.0.0.329 available for those installations that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 20.0.0.306 Multiple Vulnerabilities (APSB16-08)	Upgrade to Adobe Flash Player version 21.0.0.182 or later. Alternatively, Adobe has made version 18.0.0.333 available for those installations that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 21.0.0.197 Multiple Vulnerabilities (APSB16-10)	Upgrade to Adobe Flash Player version 21.0.0.213 or later. Alternatively, Adobe has made version 18.0.0.343 available for those installations that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 21.0.0.226 Multiple Vulnerabilities (APSB16-15)	Upgrade to Adobe Flash Player version 21.0.0.242 or later. Alternatively, Adobe has made version 18.0.0.352 available for those installations that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 21.0.0.242 Multiple Vulnerabilities (APSB16-18)	Upgrade to Adobe Flash Player version 22.0.0.192 or later. Alternatively, Adobe has made version 18.0.0.360 available for those installations that cannot be upgraded to the latest version.	High	3

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
Adobe Flash Player <= 22.0.0.192 Multiple Vulnerabilities (APSB16-25)	Upgrade to Adobe Flash Player version 22.0.0.209 or later. Alternatively, Adobe has made version 18.0.0.366 available for those installs that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 22.0.0.211 Multiple Vulnerabilities (APSB16-29)	Upgrade to Adobe Flash Player version 23.0.0.162 or later. Alternatively, Adobe has made version 18.0.0.375 available for those installs that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 23.0.0.162 Multiple Vulnerabilities (APSB16-32)	Upgrade to Adobe Flash Player version 23.0.0.185 or later. Alternatively, Adobe has made version 18.0.0.382 available for those installs that cannot be upgraded to the latest version.	High	3
Adobe Flash Player <= 23.0.0.185 Arbitrary Code Execution (APSB16-36)	Upgrade to Adobe Flash Player version 23.0.0.205 or later.	High	3
Adobe Flash Player <= 23.0.0.205 Multiple Vulnerabilities (APSB16-37)	Upgrade to Adobe Flash Player version 23.0.0.207 or later.	High	3
Adobe Flash Player <= 23.0.0.207 Multiple Vulnerabilities (APSB16-39)	Upgrade to Adobe Flash Player version 24.0.0.186 or later.	High	3
Adobe Flash Player <= 24.0.0.186 Multiple Vulnerabilities (APSB17-02)	Upgrade to Adobe Flash Player version 24.0.0.194 or later.	High	3
Adobe Flash Player <= 24.0.0.194 Multiple Vulnerabilities (APSB17-04)	Upgrade to Adobe Flash Player version 24.0.0.221 or later.	High	4
Adobe Reader < 10.1.11 / 11.0.08 Sandbox Bypass (APSB14-19)	Upgrade to Adobe Reader 10.1.11 / 11.0.08 or later.	High	1
Adobe Reader < 10.1.12 / 11.0.09 Multiple Vulnerabilities (APSB14-20)	Upgrade to Adobe Reader 10.1.12 / 11.0.09 or later.	High	1
Adobe Reader < 10.1.13 / 11.0.10 Multiple Vulnerabilities (APSB14-28)	Upgrade to Adobe Reader 10.1.13 / 11.0.10 or later.	High	1
Adobe Reader < 10.1.14 / 11.0.11 Multiple Vulnerabilities (APSB15-10)	Upgrade to Adobe Reader 10.1.14 / 11.0.11 or later.	High	1
Adobe Reader < 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-15)	Upgrade to Adobe Reader 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 or later.	High	1
Adobe Reader <= 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-24)	Upgrade to Adobe Reader 10.1.16 / 11.0.13 / 2015.006.30094 / 2015.009.20069 or later.	High	1
Adobe Reader < 10.1.9 / 11.0.6 Multiple Vulnerabilities (APSB14-01)	Upgrade to Adobe Reader 10.1.9 / 11.0.6 or later.	High	1

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
Adobe Reader < 11.0.14 / 15.006.30119 / 15.010.20056 Multiple Vulnerabilities (APSB16-02)	Upgrade to Adobe Reader 11.0.14 / 15.006.30119 / 15.010.20056 or later.	High	1
Adobe Reader < 11.0.3 / 10.1.7 / 9.5.5 Multiple Vulnerabilities (APSB13-15)	Upgrade to Adobe Reader 11.0.3 / 10.1.7 / 9.5.5 or later.	High	1
Adobe Reader < 11.0.4 / 10.1.8 Multiple Vulnerabilities (APSB13-22)	Upgrade to Adobe Reader 11.0.4 / 10.1.8 or later.	High	1
Adobe Reader < 11.0.15 / 15.006.30121 / 15.010.20060 Multiple Vulnerabilities (APSB16-09)	Upgrade to Adobe Reader version 11.0.15 / 15.006.30121 / 15.010.20060 or later.	High	1
Adobe Reader < 11.0.16 / 15.006.30172 / 15.016.20039 Multiple Vulnerabilities (APSB16-14)	Upgrade to Adobe Reader version 11.0.16 / 15.006.30172 / 15.016.20039 or later.	High	1
Adobe Reader < 11.0.17 / 15.006.30198 / 15.017.20050 Multiple Vulnerabilities (APSB16-26)	Upgrade to Adobe Reader version 11.0.17 / 15.006.30198 / 15.017.20050 or later.	High	1
Adobe Reader < 11.0.18 / 15.006.30243 / 15.020.20039 Multiple Vulnerabilities (APSB16-33)	Upgrade to Adobe Reader version 11.0.18 / 15.006.30243 / 15.020.20039 or later.	High	1
Adobe Reader < 11.0.19 / 15.006.30279 / 15.023.20053 Multiple Vulnerabilities (APSB17-01)	Upgrade to Adobe Reader version 11.0.19 / 15.006.30279 / 15.023.20053 or later.	High	1
Apache OpenOffice < 4.0 Multiple Memory Corruption Vulnerabilities	Upgrade to Apache OpenOffice version 4.0 or later.	High	1
Apache OpenOffice < 4.1.1 Multiple Vulnerabilities	Upgrade to Apache OpenOffice version 4.1.1 or later.	High	1
Apache OpenOffice < 4.1.2 Multiple Vulnerabilities	Upgrade to Apache OpenOffice version 4.1.2 or later.	High	1
Apache OpenOffice < 4.1.3 Multiple Vulnerabilities	Upgrade to Apache OpenOffice version 4.1.3 or later. Alternatively, the vendor has released a hotfix for 4.1.2 that resolves CVE-2016-1513. Note that the hotfix only resolves this one vulnerability.	High	1
Cisco WebEx for Internet Explorer RCE (cisco-sa-20170124-webex)	Upgrade to Cisco WebEx Extension version 10031.6.2017.0126 or later.	High	3
Firefox < 38.0 Multiple Vulnerabilities	Upgrade to Firefox 38.0 or later.	High	1
Firefox < 39.0 Multiple Vulnerabilities (Logjam)	Upgrade to Firefox 39.0 or later.	High	1

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
Firefox < 40 Multiple Vulnerabilities	Upgrade to Firefox 40 or later.	High	1
Firefox < 40.0.3 Multiple Vulnerabilities	Upgrade to Firefox 40.0.3 or later.	High	1
Firefox < 41 Multiple Vulnerabilities	Upgrade to Firefox 41 or later.	High	1
Firefox < 42 Multiple Vulnerabilities	Upgrade to Firefox 42 or later.	High	1
Firefox < 43 Multiple Vulnerabilities	Upgrade to Firefox 43 or later.	High	2
Firefox < 44 Multiple Vulnerabilities	Upgrade to Firefox version 44 or later.	High	3
Firefox < 45 Multiple Vulnerabilities	Upgrade to Firefox version 45 or later.	High	3
Firefox < 46 Multiple Vulnerabilities	Upgrade to Firefox version 46 or later.	High	3
Firefox < 47 Multiple Vulnerabilities	Upgrade to Firefox version 47 or later.	High	3
Firefox < 48 Multiple Vulnerabilities	Upgrade to Firefox version 48 or later.	High	4
Foxit Reader < 7.2 Multiple Vulnerabilities	Upgrade to Foxit Reader version 7.2.0.722 or later.	High	5
Foxit Reader < 7.3.4 Multiple Vulnerabilities	Upgrade to Foxit Reader version 7.3.4 or later.	High	7
Google Chrome < 39.0.2171.99 Multiple Vulnerabilities	Upgrade to Google Chrome 39.0.2171.99 or later.	High	1
Google Chrome < 40.0.2214.111 Multiple Vulnerabilities	Upgrade to Google Chrome 40.0.2214.111 or later.	High	1
Google Chrome < 40.0.2214.91 Multiple Vulnerabilities	Upgrade to Google Chrome 40.0.2214.91 or later.	High	1
Google Chrome < 40.0.2214.93 Flash Player Multiple Remote Code Execution	Upgrade to Google Chrome 40.0.2214.93 or later.	High	1
Google Chrome < 41.0.2272.118 Multiple Vulnerabilities	Upgrade to Google Chrome 41.0.2272.118 or later.	High	1
Google Chrome < 41.0.2272.76 Multiple Vulnerabilities	Upgrade to Google Chrome 41.0.2272.76 or later.	High	1
Google Chrome < 42.0.2311.135 Multiple Vulnerabilities	Upgrade to Google Chrome 42.0.2311.135 or later.	High	1
Google Chrome < 42.0.2311.152 Multiple Vulnerabilities	Upgrade to Google Chrome 42.0.2311.152 or later.	High	1
Google Chrome < 42.0.2311.90 Multiple Vulnerabilities	Upgrade to Google Chrome 42.0.2311.90 or later.	High	1
Google Chrome < 43.0.2357.124 Multiple Vulnerabilities	Upgrade to Google Chrome 43.0.2357.124 or later.	High	1
Google Chrome < 43.0.2357.132 Multiple Vulnerabilities	Upgrade to Google Chrome 43.0.2357.132 or later.	High	1

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
Google Chrome < 43.0.2357.134 Multiple RCE Vulnerabilities	Upgrade to Google Chrome 43.0.2357.134 or later.	High	1
Google Chrome < 43.0.2357.65 Multiple Vulnerabilities	Upgrade to Google Chrome 43.0.2357.65 or later.	High	1
Google Chrome < 44.0.2403.155 Multiple Vulnerabilities	Upgrade to Google Chrome 44.0.2403.155 or later.	High	1
Google Chrome < 44.0.2403.89 Multiple Vulnerabilities	Upgrade to Google Chrome 44.0.2403.89 or later.	High	1
Google Chrome < 45.0.2454.101 Multiple Vulnerabilities	Upgrade to Google Chrome 45.0.2454.101 or later.	High	1
Google Chrome < 45.0.2454.85 Multiple Vulnerabilities	Upgrade to Google Chrome 45.0.2454.85 or later.	High	1
Google Chrome < 45.0.2454.99 Multiple Vulnerabilities	Upgrade to Google Chrome 45.0.2454.99 or later.	High	1
Google Chrome < 46.0.2490.71 Multiple Vulnerabilities	Upgrade to Google Chrome 46.0.2490.71 or later.	High	1
Google Chrome < 46.0.2490.80 Multiple Vulnerabilities	Upgrade to Google Chrome 46.0.2490.80 or later.	High	1
Google Chrome < 46.0.2490.86 Multiple Vulnerabilities	Upgrade to Google Chrome 46.0.2490.86 or later.	High	1
Google Chrome < 47.0.2526.73 Multiple Vulnerabilities	Upgrade to Google Chrome 47.0.2526.73 or later.	High	1
Google Chrome < 47.0.2526.80 Multiple Vulnerabilities	Upgrade to Google Chrome 47.0.2526.80 or later.	High	1
Google Chrome < 47.0.2526.106 Multiple RCE	Upgrade to Google Chrome version 47.0.2526.106 or later.	High	1
Google Chrome < 48.0.2564.109 Multiple Vulnerabilities	Upgrade to Google Chrome version 48.0.2564.109 or later.	High	1
Google Chrome < 48.0.2564.116 Blink Same-Origin Policy Bypass	Upgrade to Google Chrome version 48.0.2564.116 or later.	High	1
Google Chrome < 48.0.2564.82 Multiple Vulnerabilities	Upgrade to Google Chrome version 48.0.2564.82 or later.	High	1
Google Chrome < 49.0.2623.108 Multiple Vulnerabilities	Upgrade to Google Chrome version 49.0.2623.108 or later.	High	1
Google Chrome < 49.0.2623.75 Multiple Vulnerabilities	Upgrade to Google Chrome version 49.0.2623.75 or later.	High	1

Vulnerability Assessment & Compliance Report

Description	Remediation	Severity	Count
Google Chrome < 49.0.2623.87 Multiple RCE	Upgrade to Google Chrome version 49.0.2623.87 or later.	High	1
Google Chrome < 50.0.2661.102 Multiple Vulnerabilities	Upgrade to Google Chrome version 50.0.2661.102 or later.	High	1
Google Chrome < 50.0.2661.75 Multiple Vulnerabilities	Upgrade to Google Chrome version 50.0.2661.75 or later.	High	1
Google Chrome < 50.0.2661.94 Multiple Vulnerabilities	Upgrade to Google Chrome version 50.0.2661.94 or later.	High	1
Google Chrome < 51.0.2704.103 Multiple Vulnerabilities	Upgrade to Google Chrome version 51.0.2704.103 or later.	High	1
Google Chrome < 51.0.2704.63 Multiple Vulnerabilities	Upgrade to Google Chrome version 51.0.2704.63 or later.	High	1
Google Chrome < 51.0.2704.79 Multiple Vulnerabilities	Upgrade to Google Chrome version 51.0.2704.79 or later.	High	1
Google Chrome < 52.0.2743.116 Multiple Vulnerabilities	Upgrade to Google Chrome version 52.0.2743.116 or later.	High	1
Google Chrome < 52.0.2743.82 Multiple Vulnerabilities	Upgrade to Google Chrome version 52.0.2743.82 or later.	High	1
Google Chrome < 53.0.2785.113 Multiple Vulnerabilities	Upgrade to Google Chrome version 53.0.2785.113 or later.	High	1
Google Chrome < 53.0.2785.143 Multiple Vulnerabilities	Upgrade to Google Chrome version 53.0.2785.143 or later.	High	1