

Data Breach Risk Scan

Assessment completed on: 201

IP: 10.211.55.3

Hostname:

OS: Windows 8.1

Unprotected Data Summary

FAIL



Unprotected Data Count by Type

Visa Credit Card	11
Social Security Number	10
Discover Credit Card	7
Diners Credit Card	9
Date of Birth	1
ACH Data	32
Visa 13 digit Credit Card	6
JCB Credit Card	9
Driver Licenses	4
Mastercard Credit Card	7
American Express Credit Card	11

Potential Liability

\$ 21,507.00

Elapsed Time	0 hours, 1 minutes, 35 seconds
Files Scanned	1,882
Files with Violation	19
Total Violations	107

Vulnerability Summary

FAIL



Vulnerability Count by Severity

High: 108
Medium: 24
Low: 8

Percentage of Vulnerabilities by Vendor

Vendor	%
Microsoft	72%
Adobe	20%
Novell	2%
Mozilla	5%

Unprotected Data Details

The findings data from your scan has been reduced to the following amounts where necessary:

*Suspected Instances: 400
Findings per Instance: 50
Folders per PST File: 50
Messages per PST Folder: 100
Files per ZIP File: 100*

File Name

Findings Count

C:\Users\ .Desktop\MLB Trade Discussions.txt

3

SHA256	f6ba740bcb10e2a109d62c772c77b6add8b73b9039c92bbb02eb1ce98b7cd570
SHA1	f244cceda0f100ed8aae1c41279cec1b318a80c1
MD5	c55e601155b5906c976a4af0c806e913

Social Security Number

476-XXXXXXXX0081

Driver Licenses

DrivXXXXXXXX8082

Visa Credit Card

4111XXXXXXXX1111

C:\Users\ .Desktop\pst_files\backup.pst

14

SHA256	361f0b50ef0b72adf1ac4f4c112616dbc0101020abb9e5d40a8b69d06f86fede
SHA1	71bc77118b3673fb36cddec96cde3bd6aa84094c
MD5	ae3925c330355b99f94563ffa4240a09

Folder: Inbox

Subject: Fw: hey can you charge these cards?

From: cbanzhof@iscanonline.com

Received: 2014-12-17 15:08:46

American Express Credit Card

3782XXXXXXXX0005

3714XXXXXXXX8431

3787XXXXXXXX1000

JCB Credit Card

3530XXXXXXXX0000

3566XXXXXXXX0505

Discover Credit Card

6011XXXXXXXX1117

6011XXXXXXXX9424

Visa Credit Card

4111XXXXXXXX1111

4012XXXXXXXX1881

Mastercard Credit Card

5555XXXXXXXX4444

5105XXXXXXXX5100

Diners Credit Card

3056XXXXXXXX5904

3852XXXXXXXX3237

Visa 13 digit Credit Card

4222XXXXXXXX2222

C:\Users
AT

\Desktop\REDACTED_ACH_FOR_ISCANONLINE.D

16

SHA256	4c8a032512d13bf56120080d6298a8b53d61e7deda4604d5597dfcf98ea72c77
SHA1	9a3377590e0670acefbbebf0c4b20661f68c8573
MD5	e598045d5428854cc49db5f787b49fcd

ACH Data

ACH File Info - Originating Institution Fake Bank X / Destination Federal Reserve Bank--- / Created 01/10/14 @ 17:27

ACH Transaction : Deposit Checking / Receiving Account : 2767XXXXXXXX / Name : XXXXXXXXXXXX / Amount : \$1,196.00

ACH Transaction : Deposit Checking / Receiving Account : 1988XXXXXXXX / Name : XXX XXXXXXXXXXXX / Amount : \$1,014.24

ACH Transaction : Debit Checking / Receiving Account : 0450XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$2,210.24

ACH Transaction : Deposit Checking / Receiving Account : 6860XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$690.00

ACH Transaction : Deposit Checking / Receiving Account : 6860XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$656.75

ACH Transaction : Deposit Checking / Receiving Account : 6860XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$614.22

ACH Transaction : Deposit Checking / Receiving Account : 6860XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$613.00

ACH Transaction : Debit Checking / Receiving Account : 0450XXXXXXXX / Name :
XXXXXXXXXXXXXXXXXX/ Amount : \$2,573.97

ACH Transaction : Deposit Checking / Receiving Account : 9876XXXXXXXX / Name :
XXXXXXXXXXXXXXXX / Amount : \$1,104.00

ACH Transaction : Deposit Checking / Receiving Account : 9319XXXXXXXX / Name :
XXXXXXXXXXXXXXXX / Amount : \$1,610.00

ACH Transaction : Deposit Checking / Receiving Account : 0006XXXXXXXX / Name :
XXXXXXXXXXXXXXXX / Amount : \$851.00

ACH Transaction : Deposit Checking / Receiving Account : 1535XXXXXXXX / Name :
XXXXXXXXXXXXXXXX / Amount : \$1,242.00

ACH Transaction : Debit Checking / Receiving Account : 0450XXXXXXXX / Name :
XXXXXXXXXXXXXXXXXX/ Amount : \$4,807.00

ACH Transaction : Deposit Checking / Receiving Account : 1536XXXXXXXX / Name :
XXX XXXXXXXX / Amount : \$175.00

ACH Transaction : Debit Checking / Receiving Account : 0450XXXXXXXX / Name :
XXXXXXXXXXXXXXXXXX/ Amount : \$175.00

C:\Users\
Orders.docx

\Documents\ecommerce Transactions\Web

15

SHA256	04d91d0c59d858ef4a006c18e884b00c56672bdde9ac1a7380d389d1217172cf
SHA1	669f9eb1ef6bbf413fba65f34d7f029795b53519
MD5	82b8693252dbaab76bcd3c3672c61b1c

American Express Credit Card

3782XXXXXXXX0005

3714XXXXXXXX8431

3787XXXXXXXX1000

JCB Credit Card

3530XXXXXXXX0000

3566XXXXXXXX0505

Visa 13 digit Credit Card

4222XXXXXXXX2222

Discover Credit Card

6011XXXXXXXX1117

6011XXXXXXXX9424

Social Security Number

458-XXXXXXXX0081

Mastercard Credit Card

5555XXXXXXXX4444

5105XXXXXXXX5100

Diners Credit Card

3056XXXXXXXX5904

3852XXXXXXXX3237

Visa Credit Card

4111XXXXXXXX1111

4012XXXXXXXX1881

C:\Users\ Documents\Mergers Acquisitions\CEO Personal Investment.rtf

2

SHA256	a0503ccb4d8a9b12e6e10bbdd4a33f5e239ba2e8d53649361661581e012eff20
SHA1	323301381c7199843cebe75a41f85f64054a600a
MD5	00f29d0fcf69f878f3ba5cfb7ecad7a4

Visa Credit Card

4111XXXXXXXX1111

Date of Birth

DOB XXXXXXXX1970

C:\Users\ \Documents\MLB Confidential Trade Talks\2015 Personal Taxes.txt

4

SHA256	3d40351ca399c51bbe8bf5899a31778ba2a5beec16dd75c19e37583e432eab62
SHA1	f336853364a3b1a5d41167d40ce597489fe8c1f8
MD5	480091056372f69ce44e79d8624295a7

Social Security Number

457-XXXXXXXX0031

Driver Licenses

DL 1XXXXXXXX7732

DrivXXXXXXXX7752

Visa Credit Card

4111XXXXXXXX1111

C:\Users\ Dropbox\Customer Test Data\ACH Payment Data\REDACTED_ACH_FOR_ISCANONLINE.DAT

16

SHA256	4c8a032512d13bf56120080d6298a8b53d61e7deda4604d5597dfcf98ea72c77
SHA1	9a3377590e0670acefbbebf0c4b20661f68c8573
MD5	e598045d5428854cc49db5f787b49fcd

ACH Data

ACH File Info - Originating Institution Fake Bank X / Destination Federal Reserve Bank--- / Created 01/10/14 @ 17:27

ACH Transaction : Deposit Checking / Receiving Account : 2767XXXXXXXX / Name : XXXXXXXXXXXX / Amount : \$1,196.00

ACH Transaction : Deposit Checking / Receiving Account : 1988XXXXXXXX / Name : XXX XXXXXXXXXXXX / Amount : \$1,014.24

ACH Transaction : Debit Checking / Receiving Account : 0450XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$2,210.24

ACH Transaction : Deposit Checking / Receiving Account : 6860XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$690.00

ACH Transaction : Deposit Checking / Receiving Account : 6860XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$656.75

ACH Transaction : Deposit Checking / Receiving Account : 6860XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$614.22

ACH Transaction : Deposit Checking / Receiving Account : 6860XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$613.00

ACH Transaction : Debit Checking / Receiving Account : 0450XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$2,573.97

ACH Transaction : Deposit Checking / Receiving Account : 9876XXXXXXXX / Name : XXXXXXXXXXXX / Amount : \$1,104.00

ACH Transaction : Deposit Checking / Receiving Account : 9319XXXXXXXX / Name : XXXXXXXXXXXX / Amount : \$1,610.00

ACH Transaction : Deposit Checking / Receiving Account : 0006XXXXXXXX / Name : XXXXXXXXXXXX / Amount : \$851.00

ACH Transaction : Deposit Checking / Receiving Account : 1535XXXXXXXX / Name : XXXXXXXXXXXX / Amount : \$1,242.00

ACH Transaction : Debit Checking / Receiving Account : 0450XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$4,807.00

ACH Transaction : Deposit Checking / Receiving Account : 1536XXXXXXXX / Name : XXX XXXXXXXX / Amount : \$175.00

ACH Transaction : Debit Checking / Receiving Account : 0450XXXXXXXX / Name : XXXXXXXXXXXXXXXXXXXX / Amount : \$175.00

C:\Users\... \Dropbox\Customer Test Data\Backup Exchange\backup.pst

14

SHA256	361f0b50ef0b72adf1ac4f4c112616dbc0101020abb9e5d40a8b69d06f86fede
SHA1	71bc77118b3673fb36cddec96cde3bd6aa84094c
MD5	ae3925c330355b99f94563ffa4240a09

Folder: Inbox

Subject: Fw: hey can you charge these cards?

From: cbanzhof@iscanonline.com

Received: 2014-12-17 15:08:46

American Express Credit Card

3782XXXXXXXX0005

3714XXXXXXXX8431

3787XXXXXXXX1000

JCB Credit Card

3530XXXXXXXX0000

3566XXXXXXXX0505

Discover Credit Card

6011XXXXXXXX1117

6011XXXXXXXX9424

Visa Credit Card

4111XXXXXXXX1111

4012XXXXXXXX1881

Mastercard Credit Card

5555XXXXXXXX4444

5105XXXXXXXX5100

Diners Credit Card

3056XXXXXXXX5904

3852XXXXXXXX3237

Visa 13 digit Credit Card

4222XXXXXXXX2222

C:\Users\... \Dropbox\Customer W9 Forms\2014 W9s.xlsx

2

SHA256	4a6731c58f4d7b2a45e653fce7f245e052fb78c0703c36486f31a286f671a160
SHA1	50cd0e42ff47d646d3546d486fb0d3079d137d47
MD5	ee643f71ba9dd4852a7e61561b61a26a

Driver Licenses

dln XXXXXXXX6683

Social Security Number

387-XXXXXXXX0041

C:\Users\... \Dropbox\Excel 2013 for Win7 CSV.csv

3

SHA256	9b1a81411b53b8bae6939d4cc95f3c729134ed189f825c10a6ffed7dfe859bb4
--------	--

SHA1	3543adfd0697814a38f0d86ad779d72478096d7
MD5	c359406b007de854c9e2d9beeb026c4d

Social Security Number

457-XXXXXXXX5462

JCB Credit Card

3530XXXXXXXX0000

Visa 13 digit Credit Card

4222XXXXXXXX0000

C:\Users\ \Dropbox\Gaming Customers IDs.xlsx 2

SHA256	986ad37821958366d4197c4113e8443446b57157425ac9ff2fe131f011e0da51
SHA1	be331cdaf3118a50936a67320fa8412beb95f2cc
MD5	7c7ed4edd5e862d1e7edaebe4164b5a1

Social Security Number

489-XXXXXXXX2283

576-XXXXXXXX0321

C:\Users\ \Dropbox\Payment Data\CC Test Data.docx 1

SHA256	d4c01e58a9753954541678596215aba49308c423dd956a63637b4304fc1a4bab
SHA1	0864303726dcecd77723f682affbbb8ccba1a557
MD5	17ac64d592d1cf5d043252081965236a

Visa Credit Card

4111XXXXXXXX1111

C:\Users\ \Dropbox\Payment Data\CC Test Data.xlsx 3

SHA256	49cdc53d96bd9f7ca71ddfd00f9b8d28a9a4cfb8819535393ced49f68068950e
SHA1	fc36a2f77a358749609ed0bc07191f86e2f92600
MD5	a47d8e20d3affb2e4477227e65c6ff6a

JCB Credit Card

3530XXXXXXXX0000

Diners Credit Card

3056XXXXXXXX5904

Visa 13 digit Credit Card

4222XXXXXXXX2222

C:\Users\... \Dropbox\Payment Data\CC Test Data.zip 3

SHA256	5398767d0ceeb4589ed72795552ea7b578f806f0e0659c060de8a6ced0db0841
SHA1	1aef92e791ddef5386bc60862a2322b4c5173a64
MD5	39323af5329681df6d430bd181f80c48

/CC Test Data.xlsx

JCB Credit Card

3530XXXXXXXX0000

Diners Credit Card

3056XXXXXXXX5904

Visa 13 digit Credit Card

4222XXXXXXXX2222

C:\Users\... \Dropbox\Web Orders\Feb Transactions.docx 4

SHA256	c2923b2eaa948b9f5fa8615bac56656dea720a82c555b34ee1bd615dd0f58b24
SHA1	05811667d751bdf970a1de532b1b03e1deec5a0
MD5	046d557f882e6f7deeb2db777569869e

Visa Credit Card

4111XXXXXXXX1111

Mastercard Credit Card

5555XXXXXXXX4444

Social Security Number

456-XXXXXXXX0081

Discover Credit Card

6011XXXXXXXX1117

C:\Users\... \Dropbox\Web Orders\Monthly sales.xlsx 2

SHA256	5752afcc01966d0f2fb971f43f5158606a904ad8101ad5fb32fdd2750738e0d9
SHA1	9e551060717f276def7c2471d05711e9edd105de
MD5	c182bd75ae5fc3a110ed5de6dc9bb602

American Express Credit Card

3782XXXXXXXX0005

Diners Credit Card

3852XXXXXXXX3237

C:\Users\ [redacted] \Dropbox\Web Orders\Online Orders.docx 1

SHA256	80e272c4c5d09c143ec082b366c37feacd6920eeef4b56abf58bf1aea542c2a1
SHA1	12aa64d501afa644f3b5811e66188fecdccd15b2
MD5	8637c61c2db81ddb01f14c08243b9f25

American Express Credit Card

3787XXXXXXXX1000

C:\Users\ [redacted] \OneDrive\Documents\Employee File.xlsx 1

SHA256	66e1a80bb2c30f1cc8b8f2fc2c67d874db70f7d96f3b0e5b540c387d013f8580
SHA1	7fc2d9f854bbc01b5ada6cb9fc1905dd0dff05d
MD5	3a8544f49e36032aa67afc78849c0ca1

Social Security Number

458-XXXXXXXX0031

C:\Users\ [redacted] \OneDrive\Documents\HR Files.zip 1

SHA256	69c4ab03e5fd745be0b56d7bdf3c2ba98dac510fc11f1ac4321073f9172ee15d
SHA1	7743d88c539df644b4043c99e4655b9d128adb47
MD5	275b11c73d8df518c600dd59282a9e30

/Employee File.xlsx

Social Security Number

458-XXXXXXXX0031

Unprotected Data Scan Statistics

Elapsed Time	0 hours, 1 minutes, 35 seconds		
Files Scanned	1,882		
Files with Suspect Data	19		
Bytes Scanned	622,295,190		
Suspected Instances Found	107		
Volumes Scanned			
Drive Root	Drive Capacity	Used Space	Free Space
C:\	68,350,373,888	14,912,847,872	53,437,526,016

Vulnerability by Vendor Details

Each vulnerability is assigned a severity level of High, Medium, or Low, which is based on the CVSS scoring system.

Severity	CVSS Score
High	7.0 - 10.0
Medium	4.0 - 6.9
Low	0.0 - 3.9

Microsoft

How to fix: *Run Windows Update to ensure you have the latest patches installed. Windows Update should be set to receive updates for 'Windows and other products from Microsoft Update.'*

Title: MS15-052 - Vulnerability in Windows Kernel Could Allow Security Feature Bypass

Check ID: lua:com.iscanonline:def:5583

CVSS: 1.9

References: CVE-2015-1674, MS15-052

Title: MS15-005 - Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass

Check ID: lua:com.iscanonline:def:5352

CVSS: 6.1

References: CVE-2015-0006, MS15-005

Title: MS15-032 - Cumulative Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5484

CVSS: 9.3

References: CVE-2015-1652, CVE-2015-1657, CVE-2015-1659, CVE-2015-1661, CVE-2015-1662, CVE-2015-1665, CVE-2015-1666, CVE-2015-1667, CVE-2015-1668, MS15-032

Title: MS14-041 - Vulnerability in DirectShow Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:5121

CVSS: 6.9

References: CVE-2014-2780, MS14-041

Title: MS14-057 - Vulnerabilities in .NET Framework Could Allow Remote Code Execution (4.5 / 4.5.1 / 4.5.2)

Check ID: lua:com.iscanonline:def:5242

CVSS: 10.0

References: CVE-2014-4073, CVE-2014-4121, MS14-057

Title: MS15-011 - Vulnerability in Group Policy Could Allow Remote Code Execution

Check ID: lua:com.iscanonline:def:5374

CVSS: 8.3

References: CVE-2015-0008, MS15-011

Title: MS14-064 - Vulnerability in Windows OLE Could Allow Remote Code Execution

Check ID: lua:com.iscanonline:def:5264

CVSS: 9.3

References: CVE-2014-6332, CVE-2014-6352, MS14-064

Title: MS14-027 - Vulnerability in Windows Shell Handler Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:5033

CVSS: 7.2

References: CVE-2014-1807, MS14-027

Title: MS14-067 - Vulnerability in XML Core Services Could Allow Remote Code Execution

Check ID: lua:com.iscanonline:def:5275

CVSS: 9.3

References: CVE-2014-4118, MS14-067

Title: MS14-072 - Vulnerability in .NET Framework Could Allow Elevation of Privilege (4.5 / 4.5.1 / 4.5.2)

Check ID: lua:com.iscanonline:def:5286

CVSS: 9.3

References: CVE-2014-4149, MS14-072

Title: MS15-077 - Vulnerability in ATM Font Driver Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:6034

CVSS: 7.2

References: CVE-2015-2387, MS15-077

Title: MS14-051 - Cumulative Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5187

CVSS: 9.3

References: CVE-2014-2774, CVE-2014-2784, CVE-2014-2796, CVE-2014-2808, CVE-2014-2810, CVE-2014-2811, CVE-2014-2817, CVE-2014-2819, CVE-2014-2820, CVE-2014-2822, CVE-2014-2823, CVE-2014-2825, CVE-2014-2826, CVE-2014-2827, CVE-2014-4050, CVE-2014-4051, CVE-2014-4055, CVE-2014-4057, CVE-2014-4058, CVE-2014-4063, CVE-2014-4067, MS14-051

Title: MS14-036 - Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (gdi32, usp10, dwrite)

Check ID: lua:com.iscanonline:def:5088

CVSS: 9.3

References: CVE-2014-1817, CVE-2014-1818, MS14-036

Title: MS15-028 - Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass

Check ID: lua:com.iscanonline:def:5430

CVSS: 2.1

References: CVE-2015-0084, MS15-028

Title: MS15-006 - Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass

Check ID: lua:com.iscanonline:def:5353

CVSS: 1.9

References: CVE-2015-0001, MS15-006

Title: MS14-058 - Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution

Check ID: lua:com.iscanonline:def:5243

CVSS: 9.3

References: CVE-2014-4113, CVE-2014-4148, MS14-058

Title: MS15-085 - Vulnerability in Mount Manager Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:6123

CVSS: 7.2

References: CVE-2015-1769, MS15-085

Title: MS14-049 - Vulnerability in Windows Installer Service Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:5177

CVSS: 7.2

References: CVE-2014-1814, MS14-049

Title:	MS15-051 - Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege
Check ID:	lua:com.iscanonline:def:5530
CVSS:	2.1
References:	CVE-2015-1676, CVE-2015-1677, CVE-2015-1678, CVE-2015-1679, CVE-2015-1680, MS15-051
Title:	MS15-029 - Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure
Check ID:	lua:com.iscanonline:def:5431
CVSS:	4.3
References:	CVE-2015-0076, MS15-029
Title:	MS14-060 - Vulnerability in Windows OLE Could Allow Remote Code Execution
Check ID:	lua:com.iscanonline:def:5244
CVSS:	9.3
References:	CVE-2014-4114, MS14-060
Title:	MS15-014 - Vulnerability in Group Policy Could Allow Security Feature Bypass
Check ID:	lua:com.iscanonline:def:5398
CVSS:	3.3
References:	CVE-2015-0009, MS15-014
Title:	MS14-026 - Vulnerability in .NET Framework Could Allow Elevation of Privilege (4.5 / 4.5.1)
Check ID:	lua:com.iscanonline:def:5046
CVSS:	10.0
References:	CVE-2014-1806, MS14-026
Title:	MS14-074 - Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass
Check ID:	lua:com.iscanonline:def:5288
CVSS:	5.0
References:	CVE-2014-6318, MS14-074
Title:	MS14-068 - Vulnerability in Kerberos Could Allow Elevation of Privilege
Check ID:	lua:com.iscanonline:def:5299
CVSS:	9.0
References:	CVE-2014-6324, MS14-068
Title:	MS15-078 - Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution
Check ID:	lua:com.iscanonline:def:6047
CVSS:	9.3
References:	CVE-2015-2426, MS15-078

Title:	MS15-020 - Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution
Check ID:	lua:com.iscanonline:def:5421
CVSS:	9.3
References:	CVE-2015-0081, CVE-2015-0096, MS15-020
Title:	MS15-030 - Vulnerability in Remote Desktop Protocol Could Allow Denial of Service
Check ID:	lua:com.iscanonline:def:5432
CVSS:	7.8
References:	CVE-2015-0079, MS15-030
Title:	MS15-054 - Vulnerability in Microsoft Management Console File Format Could Allow Denial of Service
Check ID:	lua:com.iscanonline:def:5586
CVSS:	1.9
References:	CVE-2015-1681, MS15-054
Title:	MS15-008 - Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege
Check ID:	lua:com.iscanonline:def:5355
CVSS:	4.7
References:	CVE-2015-0011, MS15-008
Title:	MS15-034 - Vulnerability in HTTP.sys Could Allow Remote Code Execution
Check ID:	lua:com.iscanonline:def:5498
CVSS:	10.0
References:	CVE-2015-1635, MS15-034
Title:	MS15-015 - Vulnerability in Microsoft Windows Could Allow Elevation of Privilege
Check ID:	lua:com.iscanonline:def:5399
CVSS:	7.2
References:	CVE-2015-0062, MS15-015
Title:	MS15-021 - Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution
Check ID:	lua:com.iscanonline:def:5422
CVSS:	9.3
References:	CVE-2015-0074, CVE-2015-0087, CVE-2015-0088, CVE-2015-0089, CVE-2015-0090, CVE-2015-0091, CVE-2015-0092, CVE-2015-0093, MS15-021
Title:	MS15-031 - Vulnerability in Schannel Could Allow Security Feature Bypass
Check ID:	lua:com.iscanonline:def:5433
CVSS:	4.3
References:	CVE-2015-1637, MS15-031

Title:	MS15-055 - Vulnerability in Schannel Could Allow Information Disclosure
Check ID:	lua:com.iscanonline:def:5587
CVSS:	5.0
References:	CVE-2015-1716, MS15-055
Title:	MS14-045 - Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (GDI)
Check ID:	lua:com.iscanonline:def:5169
CVSS:	7.2
References:	CVE-2014-0318, CVE-2014-1819, CVE-2014-4064, MS14-045
Title:	MS15-016 - Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (windowscodecs.dll)
Check ID:	lua:com.iscanonline:def:5401
CVSS:	4.3
References:	CVE-2015-0061, MS15-016
Title:	MS15-023 - Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
Check ID:	lua:com.iscanonline:def:5423
CVSS:	7.2
References:	CVE-2015-0077, CVE-2015-0078, CVE-2015-0094, CVE-2015-0095, MS15-023
Title:	MS14-053 - Vulnerability in .NET Framework Could Allow Denial of Service (4.5 / 4.5.1 / 4.5.2)
Check ID:	lua:com.iscanonline:def:5214
CVSS:	5.0
References:	CVE-2014-4072, MS14-053
Title:	MS15-088 - Unsafe Command Line Parameter Passing Could Allow Information Disclosure
Check ID:	lua:com.iscanonline:def:6127
CVSS:	4.3
References:	CVE-2015-2423, MS15-088
Title:	MS15-094 - Cumulative Security Update for Internet Explorer 11
Check ID:	lua:com.iscanonline:def:6149
CVSS:	9.3
References:	CVE-2015-2483, CVE-2015-2484, CVE-2015-2485, CVE-2015-2486, CVE-2015-2487, CVE-2015-2489, CVE-2015-2490, CVE-2015-2491, CVE-2015-2492, CVE-2015-2494, CVE-2015-2498, CVE-2015-2499, CVE-2015-2541, CVE-2015-2542, MS15-094
Title:	MS15-041 - Vulnerability in .NET Framework Could Allow Information Disclosure (4.5 / 4.5.1 / 4.5.2)
Check ID:	lua:com.iscanonline:def:5512
CVSS:	2.6

References: CVE-2015-1648, MS15-041

Title: MS14-054 - Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:5215

CVSS: 6.8

References: CVE-2014-4074, MS14-054

Title: MS14-056 - Cumulative Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5237

CVSS: 9.3

References: CVE-2014-4123, CVE-2014-4124, CVE-2014-4126, CVE-2014-4128, CVE-2014-4130, CVE-2014-4132, CVE-2014-4138, CVE-2014-4140, CVE-2014-4141, MS14-056

Title: MS14-021 - Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5017

CVSS: 10.0

References: CVE-2014-1776, MS14-021

Title: MS15-089 - Vulnerability in WebDAV Could Allow Information Disclosure

Check ID: lua:com.iscanonline:def:6128

CVSS: 2.6

References: CVE-2015-2476, MS15-089

Title: MS15-072 - Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:6029

CVSS: 7.2

References: CVE-2015-2364, MS15-072

Title: MS15-060 - Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution

Check ID: lua:com.iscanonline:def:5865

CVSS: 9.3

References: CVE-2015-1756, MS15-060

Title: MS15-065 - Cumulative Security Update for Internet Explorer 11 (KB3074886)

Check ID: lua:com.iscanonline:def:5997

CVSS: 9.3

References: CVE-2015-1729, CVE-2015-1733, CVE-2015-1767, CVE-2015-2372, CVE-2015-2383, CVE-2015-2384, CVE-2015-2385, CVE-2015-2389, CVE-2015-2390, CVE-2015-2397, CVE-2015-2398, CVE-2015-2401, CVE-2015-2402, CVE-2015-2404, CVE-2015-2406, CVE-2015-2408, CVE-2015-2410, CVE-2015-2411, CVE-2015-2412, CVE-2015-2413, CVE-2015-2414, CVE-2015-2419, CVE-2015-2421, CVE-2015-2422, CVE-2015-2425, MS15-065

Title:	MS15-024 - Vulnerability in PNG Processing Could Allow Information Disclosure (windowscodecs.dll)
Check ID:	lua:com.iscanonline:def:5425
CVSS:	4.3
References:	CVE-2015-0080, MS15-024
Title:	MS15-001 - Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege
Check ID:	lua:com.iscanonline:def:5348
CVSS:	7.2
References:	CVE-2015-0002, MS15-001
Title:	MS15-082 - Vulnerabilities in RDP Could Allow Remote Code Execution
Check ID:	lua:com.iscanonline:def:6118
CVSS:	4.3
References:	CVE-2015-2472, MS15-082
Title:	MS15-090 - Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege
Check ID:	lua:com.iscanonline:def:6129
CVSS:	9.3
References:	CVE-2015-2428, CVE-2015-2429, CVE-2015-2430, MS15-090
Title:	MS15-061 - Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
Check ID:	lua:com.iscanonline:def:5866
CVSS:	7.2
References:	CVE-2015-1719, CVE-2015-1720, CVE-2015-1721, CVE-2015-1722, CVE-2015-1723, CVE-2015-1724, CVE-2015-1725, CVE-2015-1726, CVE-2015-1727, CVE-2015-2360, MS15-061
Title:	MS15-025 - Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege
Check ID:	lua:com.iscanonline:def:5426
CVSS:	7.2
References:	CVE-2015-0073, MS15-025
Title:	MS15-045 - Vulnerability in Windows Journal Could Allow Remote Code Execution
Check ID:	lua:com.iscanonline:def:5547
CVSS:	9.3
References:	CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, CVE-2015-1698, CVE-2015-1699, MS15-045
Title:	MS14-085 - Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (windowscodecs.dll)
Check ID:	lua:com.iscanonline:def:5338

CVSS: 5.0

References: CVE-2014-6355, MS14-085

Title: MS15-056 - Cumulative Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5856

CVSS: 9.3

References: CVE-2015-1731, CVE-2015-1732, CVE-2015-1735, CVE-2015-1736, CVE-2015-1737, CVE-2015-1739, CVE-2015-1740, CVE-2015-1741, CVE-2015-1742, CVE-2015-1743, CVE-2015-1744, CVE-2015-1745, CVE-2015-1747, CVE-2015-1748, CVE-2015-1750, CVE-2015-1752, CVE-2015-1753, CVE-2015-1755, CVE-2015-1765, CVE-2015-1766, MS15-056

Title: MS15-038 - Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:5504

CVSS: 7.2

References: CVE-2015-1643, CVE-2015-1644, MS15-038

Title: MS15-065 - Cumulative Security Update for Internet Explorer 11 (KB3075516)

Check ID: lua:com.iscanonline:def:5999

CVSS: 9.3

References: CVE-2015-1729, CVE-2015-1733, CVE-2015-1767, CVE-2015-2372, CVE-2015-2383, CVE-2015-2384, CVE-2015-2385, CVE-2015-2389, CVE-2015-2390, CVE-2015-2397, CVE-2015-2398, CVE-2015-2401, CVE-2015-2402, CVE-2015-2404, CVE-2015-2406, CVE-2015-2408, CVE-2015-2410, CVE-2015-2411, CVE-2015-2412, CVE-2015-2413, CVE-2015-2414, CVE-2015-2419, CVE-2015-2421, CVE-2015-2422, CVE-2015-2425, MS15-065

Title: MS14-052 - Cumulative Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5207

CVSS: 9.3

References: CVE-2013-7331, CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4080, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4087, CVE-2014-4088, CVE-2014-4089, CVE-2014-4090, CVE-2014-4091, CVE-2014-4092, CVE-2014-4094, CVE-2014-4095, CVE-2014-4096, CVE-2014-4097, CVE-2014-4098, CVE-2014-4099, CVE-2014-4100, CVE-2014-4101, CVE-2014-4102, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, CVE-2014-4111, MS14-052

Title: MS15-065 - Cumulative Security Update for Internet Explorer 11 (KB3065822)

Check ID: lua:com.iscanonline:def:5989

CVSS: 9.3

References: CVE-2015-1729, CVE-2015-1733, CVE-2015-1767, CVE-2015-2372, CVE-2015-2383, CVE-2015-2384, CVE-2015-2385, CVE-2015-2389, CVE-2015-2390, CVE-2015-2397, CVE-2015-2398, CVE-2015-2401, CVE-2015-2402, CVE-2015-2404, CVE-2015-2406, CVE-2015-2408, CVE-2015-2410, CVE-2015-2411, CVE-2015-2412, CVE-2015-2413, CVE-2015-2414, CVE-2015-2419, CVE-2015-2421, CVE-2015-2422, CVE-2015-2425, MS15-065

Title: MS15-018 - Cumulative Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5417

CVSS: 9.3

References: CVE-2015-0032, CVE-2015-0056, CVE-2015-0072, CVE-2015-1622, CVE-2015-1623, CVE-2015-1624, CVE-2015-1625, CVE-2015-1626, CVE-2015-1627, CVE-2015-1634, MS15-018

Title: MS15-043 - Cumulative Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5528

CVSS: 9.3

References: CVE-2015-1658, CVE-2015-1684, CVE-2015-1685, CVE-2015-1686, CVE-2015-1688, CVE-2015-1689, CVE-2015-1692, CVE-2015-1694, CVE-2015-1703, CVE-2015-1704, CVE-2015-1705, CVE-2015-1706, CVE-2015-1709, CVE-2015-1710, CVE-2015-1711, CVE-2015-1713, CVE-2015-1714, CVE-2015-1717, CVE-2015-1718, MS15-043

Title: MS15-044 - Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution

Check ID: lua:com.iscanonline:def:5529

CVSS: 9.3

References: CVE-2015-1670, CVE-2015-1671, MS15-044

Title: MS14-080 - Cumulative Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5309

CVSS: 9.3

References: CVE-2014-6327, CVE-2014-6328, CVE-2014-6329, CVE-2014-6363, CVE-2014-6365, CVE-2014-6368, CVE-2014-6369, CVE-2014-6374, CVE-2014-6376, MS14-080

Title: MS14-035 - Cumulative Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5080

CVSS: 10.0

References: CVE-2014-0282, CVE-2014-1762, CVE-2014-1764, CVE-2014-1766, CVE-2014-1769, CVE-2014-1770, CVE-2014-1771, CVE-2014-1772, CVE-2014-1773, CVE-2014-1775, CVE-2014-1777, CVE-2014-1778, CVE-2014-1779, CVE-2014-1780, CVE-2014-1782, CVE-2014-1783, CVE-2014-1784, CVE-2014-1785, CVE-2014-1786, CVE-2014-1791, CVE-2014-1794, CVE-2014-1795, CVE-2014-1796, CVE-2014-1797, CVE-2014-1799, CVE-2014-1800, CVE-2014-1802, CVE-2014-1803, CVE-2014-1805, CVE-2014-2753, CVE-2014-2755, CVE-2014-2756, CVE-2014-2757, CVE-2014-2758, CVE-2014-2759, CVE-2014-2760, CVE-2014-2761, CVE-2014-2763, CVE-2014-2764, CVE-2014-2765, CVE-2014-2766, CVE-2014-2769, CVE-2014-2771, CVE-2014-2772, CVE-2014-2775, CVE-2014-2776, CVE-2014-2777, MS14-035

Title: MS14-071 - Vulnerability in Windows Audio Service Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:5280

CVSS: 4.3

References: CVE-2014-6322, MS14-071

Title: MS14-045 - Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (Direct X)

Check ID: lua:com.iscanonline:def:5170

CVSS: 7.2

References: CVE-2014-0318, CVE-2014-1819, CVE-2014-4064, MS14-045

Title: MS14-030 - Vulnerability in Remote Desktop Could Allow Tampering

Check ID: lua:com.iscanonline:def:5083

CVSS: 5.1

References: CVE-2014-0296, MS14-030

Title: MS14-037 - Cumulative Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5051

CVSS: 10.0

References: CVE-2014-1763, CVE-2014-1765, CVE-2014-2783, CVE-2014-2786, CVE-2014-2787, CVE-2014-2789, CVE-2014-2790, CVE-2014-2792, CVE-2014-2795, CVE-2014-2798, CVE-2014-2800, CVE-2014-2801, CVE-2014-2802, CVE-2014-2804, CVE-2014-2806, CVE-2014-2807, CVE-2014-2809, CVE-2014-2813, MS14-037

Title: MS14-079 - Vulnerability in Kernel-Mode Driver Could Allow Denial of Service

Check ID: lua:com.iscanonline:def:5293

CVSS: 7.1

References: CVE-2014-6317, MS14-079

Title: MS15-073 - Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:6030

CVSS: 7.2

References: CVE-2015-2365, CVE-2015-2366, CVE-2015-2367, CVE-2015-2381, CVE-2015-2382, MS15-073

Title: MS14-031 - Vulnerability in TCP Protocol Could Allow Denial of Service

Check ID: lua:com.iscanonline:def:5084

CVSS: 5.0

References: CVE-2014-1811, MS14-031

Title: MS15-093 - Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:6141

CVSS: 9.3

References: CVE-2015-2502, MS15-093

Title: MS14-038 - Vulnerability in Windows Journal Could Allow Remote Code Execution

Check ID: lua:com.iscanonline:def:5052

CVSS: 9.3

References: CVE-2014-1824, MS14-038

Title: MS15-074 - Vulnerability in Windows Installer Service Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:6031

CVSS: 6.9

References: CVE-2015-2371, MS15-074

Title:	MS15-098 - Vulnerabilities in Windows Journal Could Allow Remote Code Execution
Check ID:	lua:com.iscanonline:def:6163
CVSS:	9.3
References:	CVE-2015-2513, CVE-2015-2514, CVE-2015-2516, CVE-2015-2519, CVE-2015-2530, MS15-098
Title:	MS15-079 - Cumulative Security Update for Internet Explorer 11
Check ID:	lua:com.iscanonline:def:6053
CVSS:	9.3
References:	CVE-2015-2423, CVE-2015-2441, CVE-2015-2442, CVE-2015-2443, CVE-2015-2444, CVE-2015-2446, CVE-2015-2447, CVE-2015-2449, CVE-2015-2450, CVE-2015-2451, CVE-2015-2452, MS15-079
Title:	MS14-033 - Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure
Check ID:	lua:com.iscanonline:def:5085
CVSS:	4.3
References:	CVE-2014-1816, MS14-033
Title:	MS15-101 - Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (4.5/4.5.1/4.5.2)
Check ID:	lua:com.iscanonline:def:6185
CVSS:	9.3
References:	CVE-2015-2504, CVE-2015-2526, MS15-101
Title:	MS15-003 - Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege
Check ID:	lua:com.iscanonline:def:5350
CVSS:	7.2
References:	CVE-2015-0004, MS15-003
Title:	MS15-009 - Cumulative Security Update for Internet Explorer 11
Check ID:	lua:com.iscanonline:def:5372
CVSS:	9.3
References:	CVE-2015-0017, CVE-2015-0018, CVE-2015-0020, CVE-2015-0022, CVE-2015-0026, CVE-2015-0027, CVE-2015-0030, CVE-2015-0031, CVE-2015-0035, CVE-2015-0036, CVE-2015-0037, CVE-2015-0038, CVE-2015-0039, CVE-2015-0040, CVE-2015-0041, CVE-2015-0042, CVE-2015-0043, CVE-2015-0046, CVE-2015-0052, CVE-2015-0054, CVE-2015-0055, CVE-2015-0066, CVE-2015-0068, CVE-2015-0069, CVE-2015-0070, CVE-2015-0071, MS15-009
Title:	MS15-084 - Vulnerabilities in XML Core Services Could Allow Information Disclosure (XML 3.0)
Check ID:	lua:com.iscanonline:def:6120
CVSS:	4.3
References:	CVE-2015-2434, CVE-2015-2440, CVE-2015-2471, MS15-084
Title:	MS14-065 - Cumulative Security Update for Internet Explorer 11
Check ID:	lua:com.iscanonline:def:5273

CVSS: 9.3
References: CVE-2014-4143, CVE-2014-6323, CVE-2014-6337, CVE-2014-6340, CVE-2014-6341, CVE-2014-6343, CVE-2014-6346, CVE-2014-6347, CVE-2014-6349, CVE-2014-6350, CVE-2014-6351, MS14-065

Title: MS14-039 - Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:5053

CVSS: 7.6

References: CVE-2014-2781, MS14-039

Title: MS15-075 - Vulnerabilities in OLE Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:6032

CVSS: 5.0

References: CVE-2015-2416, CVE-2015-2417, MS15-075

Title: MS15-097 - Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (atmfd)

Check ID: lua:com.iscanonline:def:6153

CVSS: 9.3

References: CVE-2015-2506, CVE-2015-2507, CVE-2015-2511, CVE-2015-2512, CVE-2015-2517, CVE-2015-2518, CVE-2015-2527, CVE-2015-2529, CVE-2015-2546, MS15-097

Title: MS15-080 - Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (atmfd)

Check ID: lua:com.iscanonline:def:6054

CVSS: 9.3

References: CVE-2015-2432, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2435, CVE-2015-2455, CVE-2015-2456, CVE-2015-2463, CVE-2015-2464, CVE-2015-2433, CVE-2015-2453, CVE-2015-2454, CVE-2015-2465, MS15-080

Title: MS15-050 - Vulnerability in Service Control Manager Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:5582

CVSS: 6.9

References: CVE-2015-1702, MS15-050

Title: MS15-048 - Vulnerability in .NET Framework Could Allow Information Disclosure (4.5 / 4.5.1 / 4.5.2)

Check ID: lua:com.iscanonline:def:5593

CVSS: 9.3

References: CVE-2015-1672, CVE-2015-1673, MS15-048

Title: MS15-004 - Vulnerability in Windows Components Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:5351

CVSS: 9.3

References: CVE-2015-0016, MS15-004

Title: MS14-040 - Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:5120

CVSS: 7.2

References: CVE-2014-1767, MS14-040

Title: MS15-010 - Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution

Check ID: lua:com.iscanonline:def:5373

CVSS: 7.2

References: CVE-2015-0003, CVE-2015-0010, CVE-2015-0057, CVE-2015-0058, CVE-2015-0059, CVE-2015-0060, MS15-010

Title: MS15-084 - Vulnerabilities in XML Core Services Could Allow Information Disclosure (XML 6.0)

Check ID: lua:com.iscanonline:def:6121

CVSS: 4.3

References: CVE-2015-2440, MS15-084

Title: MS14-029 - Security Update for Internet Explorer 11

Check ID: lua:com.iscanonline:def:5032

CVSS: 9.3

References: CVE-2014-0310, CVE-2014-1815, MS14-029

Title: MS14-066 - Vulnerability in Schannel Could Allow Remote Code Execution

Check ID: lua:com.iscanonline:def:5274

CVSS: 10.0

References: CVE-2014-6321, MS14-066

Title: MS14-047 - Vulnerability in LRPC Could Allow Security Feature Bypass

Check ID: lua:com.iscanonline:def:5175

CVSS: 7.5

References: CVE-2014-0316, MS14-047

Title: MS15-076 - Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:6033

CVSS: 7.2

References: CVE-2015-2370, MS15-076

Title: MS15-080 - Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution

Check ID: lua:com.iscanonline:def:6055

CVSS: 9.3

References: CVE-2015-2432, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2435, CVE-2015-2455, CVE-2015-2456, CVE-2015-2463, CVE-2015-2464, CVE-2015-2433, CVE-2015-2453, CVE-2015-2454, CVE-2015-2465, MS15-080

Title: MS15-102 - Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege

Check ID: lua:com.iscanonline:def:6187

CVSS: 7.2

References: CVE-2015-2524, CVE-2015-2525, CVE-2015-2528, MS15-102

Adobe

How to fix: *Run the affected software's update mechanism, or go to the vendor's site to download the latest version and/or patches.*

Title: APSB15-09 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5594

CVSS: 10.0

References: CVE-2015-3044, CVE-2015-3077, CVE-2015-3078, CVE-2015-3079, CVE-2015-3080, CVE-2015-3081, CVE-2015-3082, CVE-2015-3083, CVE-2015-3084, CVE-2015-3085, CVE-2015-3086, CVE-2015-3087, CVE-2015-3088, CVE-2015-3089, CVE-2015-3090, CVE-2015-3091, CVE-2015-3092, CVE-2015-3093, APSB15-09

Title: APSB15-09 - Security Update for Adobe AIR

Check ID: lua:com.iscanonline:def:5595

CVSS: 10.0

References: CVE-2015-3044, CVE-2015-3077, CVE-2015-3078, CVE-2015-3079, CVE-2015-3080, CVE-2015-3081, CVE-2015-3082, CVE-2015-3083, CVE-2015-3084, CVE-2015-3085, CVE-2015-3086, CVE-2015-3087, CVE-2015-3088, CVE-2015-3089, CVE-2015-3090, CVE-2015-3091, CVE-2015-3092, CVE-2015-3093, APSB15-09

Title: APSB15-14 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:6035

CVSS: 10.0

References: CVE-2015-3113, APSB15-14

Title: APSB15-11 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5871

CVSS: 10.0

References: CVE-2015-3096, CVE-2015-3097, CVE-2015-3098, CVE-2015-3099, CVE-2015-3100, CVE-2015-3101, CVE-2015-3102, CVE-2015-3103, CVE-2015-3104, CVE-2015-3105, CVE-2015-3106, CVE-2015-3107, CVE-2015-3108, APSB15-11

Title: APSB14-26 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5343

CVSS: 10.0

References: CVE-2014-8439, APSB14-26

Title: APSB15-05 - Security Update for Adobe AIR

Check ID: lua:com.iscanonline:def:5596

CVSS: 10.0

References: CVE-2015-0332, CVE-2015-0333, CVE-2015-0334, CVE-2015-0335, CVE-2015-0336, CVE-2015-0337, CVE-2015-0338, CVE-2015-0339, CVE-2015-0340, CVE-2015-0341, CVE-2015-0342, APSB15-05

Title: APSB15-11 - Security Update for Adobe AIR

Check ID: lua:com.iscanonline:def:5872

CVSS: 10.0

References: CVE-2015-3096, CVE-2015-3097, CVE-2015-3098, CVE-2015-3099, CVE-2015-3100, CVE-2015-3101, CVE-2015-3102, CVE-2015-3103, CVE-2015-3104, CVE-2015-3105, CVE-2015-3106, CVE-2015-3107, CVE-2015-3108, APSB15-11

Title: APSB14-27 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5344

CVSS: 10.0

References: CVE-2014-0580, CVE-2014-0587, CVE-2014-8443, CVE-2014-9162, CVE-2014-9163, CVE-2014-9164, APSB14-27

Title: APSB15-06 - Security Update for Adobe AIR

Check ID: lua:com.iscanonline:def:5597

CVSS: 10.0

References: CVE-2015-0346, CVE-2015-0347, CVE-2015-0348, CVE-2015-0349, CVE-2015-0350, CVE-2015-0351, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0356, CVE-2015-0357, CVE-2015-0358, CVE-2015-0359, CVE-2015-0360, CVE-2015-3038, CVE-2015-3039, CVE-2015-3040, CVE-2015-3041, CVE-2015-3042, CVE-2015-3043, CVE-2015-3044, APSB15-06

Title: APSB15-16 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:6037

CVSS: 10.0

References: CVE-2014-0578, CVE-2015-3097, CVE-2015-3114, CVE-2015-3115, CVE-2015-3116, CVE-2015-3117, CVE-2015-3118, CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, CVE-2015-3122, CVE-2015-3123, CVE-2015-3124, CVE-2015-3125, CVE-2015-3126, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3130, CVE-2015-3131, CVE-2015-3132, CVE-2015-3133, CVE-2015-3134, CVE-2015-3135, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4429, CVE-2015-4430, CVE-2015-4431, CVE-2015-4432, CVE-2015-4433, CVE-2015-5116, CVE-2015-5117, CVE-2015-5118, CVE-2015-5119, APSB15-16

Title: APSB15-01 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5356

CVSS: 10.0

References: CVE-2015-0301, CVE-2015-0302, CVE-2015-0303, CVE-2015-0304, CVE-2015-0305, CVE-2015-0306, CVE-2015-0307, CVE-2015-0308, CVE-2015-0309, APSB15-01

Title:	APSB14-17 - Security Update for Adobe Flash Player
Check ID:	lua:com.iscanonline:def:5136
CVSS:	7.5
References:	CVE-2014-0537, CVE-2014-0539, CVE-2014-4671, APSB14-17
Title:	APSB15-16 - Security Update for Adobe AIR
Check ID:	lua:com.iscanonline:def:6038
CVSS:	10.0
References:	CVE-2014-0578, CVE-2015-3097, CVE-2015-3114, CVE-2015-3115, CVE-2015-3116, CVE-2015-3117, CVE-2015-3118, CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, CVE-2015-3122, CVE-2015-3123, CVE-2015-3124, CVE-2015-3125, CVE-2015-3126, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3130, CVE-2015-3131, CVE-2015-3132, CVE-2015-3133, CVE-2015-3134, CVE-2015-3135, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4429, CVE-2015-4430, CVE-2015-4431, CVE-2015-4432, CVE-2015-4433, CVE-2015-5116, CVE-2015-5117, CVE-2015-5118, CVE-2015-5119, APSB15-16
Title:	APSB15-01 - Security Update for Adobe AIR
Check ID:	lua:com.iscanonline:def:5357
CVSS:	10.0
References:	CVE-2015-0301, CVE-2015-0302, CVE-2015-0303, CVE-2015-0304, CVE-2015-0305, CVE-2015-0306, CVE-2015-0307, CVE-2015-0308, CVE-2015-0309, APSB15-01
Title:	APSB14-22 - Security Update for Adobe Flash Player
Check ID:	lua:com.iscanonline:def:5258
CVSS:	10.0
References:	CVE-2014-0558, CVE-2014-0564, CVE-2014-0569, APSB14-22
Title:	APSB15-18 - Security Update for Adobe Flash Player
Check ID:	lua:com.iscanonline:def:6039
CVSS:	10.0
References:	CVE-2014-0578, CVE-2015-3097, CVE-2015-3114, CVE-2015-3115, CVE-2015-3116, CVE-2015-3117, CVE-2015-3118, CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, CVE-2015-3122, CVE-2015-3123, CVE-2015-3124, CVE-2015-3125, CVE-2015-3126, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3130, CVE-2015-3131, CVE-2015-3132, CVE-2015-3133, CVE-2015-3134, CVE-2015-3135, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4429, CVE-2015-4430, CVE-2015-4431, CVE-2015-4432, CVE-2015-4433, CVE-2015-5116, CVE-2015-5117, CVE-2015-5118, CVE-2015-5119, APSB15-18
Title:	APSB15-05 - Security Update for Adobe Flash Player
Check ID:	lua:com.iscanonline:def:5468
CVSS:	10.0
References:	CVE-2015-0332, CVE-2015-0333, CVE-2015-0334, CVE-2015-0335, CVE-2015-0336, CVE-2015-0337, CVE-2015-0338, CVE-2015-0339, CVE-2015-0340, CVE-2015-0341, CVE-2015-0342, APSB15-05
Title:	APSB15-06 - Security Update for Adobe Flash Player
Check ID:	lua:com.iscanonline:def:5513

CVSS: 10.0

References: CVE-2015-0346, CVE-2015-0347, CVE-2015-0348, CVE-2015-0349, CVE-2015-0350, CVE-2015-0351, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0356, CVE-2015-0357, CVE-2015-0358, CVE-2015-0359, CVE-2015-0360, CVE-2015-3038, CVE-2015-3039, CVE-2015-3040, CVE-2015-3041, CVE-2015-3042, CVE-2015-3043, CVE-2015-3044, APSB15-06

Title: APSB15-03 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5404

CVSS: 10.0

References: CVE-2015-0311, CVE-2015-0312, APSB15-03

Title: APSB15-04 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5405

CVSS: 10.0

References: CVE-2015-0313, CVE-2015-0314, CVE-2015-0315, CVE-2015-0316, CVE-2015-0317, CVE-2015-0318, CVE-2015-0319, CVE-2015-0320, CVE-2015-0321, CVE-2015-0322, CVE-2015-0323, CVE-2015-0324, CVE-2015-0325, CVE-2015-0326, CVE-2015-0327, CVE-2015-0328, CVE-2015-0329, CVE-2015-0330, APSB15-04

Title: APSB14-21 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5218

CVSS: 10.0

References: CVE-2014-0547, CVE-2014-0548, CVE-2014-0549, CVE-2014-0550, CVE-2014-0551, CVE-2014-0552, CVE-2014-0553, CVE-2014-0554, CVE-2014-0555, CVE-2014-0556, CVE-2014-0557, CVE-2014-0559, APSB14-21

Title: APSB14-14 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5071

CVSS: 10.0

References: CVE-2014-0510, CVE-2014-0516, CVE-2014-0517, CVE-2014-0518, CVE-2014-0519, CVE-2014-0520, APSB14-14

Title: APSB14-18 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5193

CVSS: 10.0

References: CVE-2014-0538, CVE-2014-0540, CVE-2014-0541, CVE-2014-0542, CVE-2014-0543, CVE-2014-0544, CVE-2014-0545, APSB14-18

Title: APSB14-16 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5095

CVSS: 10.0

References: CVE-2014-0531, CVE-2014-0532, CVE-2014-0533, CVE-2014-0534, CVE-2014-0535, CVE-2014-0536, APSB14-16

Title: APSB14-24 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5294
CVSS: 10.0
References: CVE-2014-0573, CVE-2014-0574, CVE-2014-0576, CVE-2014-0577, CVE-2014-0581, CVE-2014-0582, CVE-2014-0583, CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, CVE-2014-0588, CVE-2014-0589, CVE-2014-0590, CVE-2014-8437, CVE-2014-8438, CVE-2014-8440, CVE-2014-8441, CVE-2014-8442, AP SB14-24

Title: AP SB15-19 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:6131

CVSS: 10.0

References: CVE-2015-5124, CVE-2015-5125, CVE-2015-5127, CVE-2015-5129, CVE-2015-5130, CVE-2015-5131, CVE-2015-5132, CVE-2015-5133, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5541, CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5550, CVE-2015-5551, CVE-2015-5552, CVE-2015-5553, CVE-2015-5554, CVE-2015-5555, CVE-2015-5556, CVE-2015-5557, CVE-2015-5558, CVE-2015-5559, CVE-2015-5560, CVE-2015-5561, CVE-2015-5562, CVE-2015-5563, CVE-2015-5564, CVE-2015-5565, AP SB15-19

Title: AP SB15-02 - Security Update for Adobe Flash Player

Check ID: lua:com.iscanonline:def:5362

CVSS: 10.0

References: CVE-2015-0310, AP SB15-02

Title: AP SB15-19 - Security Update for Adobe AIR

Check ID: lua:com.iscanonline:def:6132

CVSS: 10.0

References: CVE-2015-5124, CVE-2015-5125, CVE-2015-5127, CVE-2015-5129, CVE-2015-5130, CVE-2015-5131, CVE-2015-5132, CVE-2015-5133, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5541, CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5550, CVE-2015-5551, CVE-2015-5552, CVE-2015-5553, CVE-2015-5554, CVE-2015-5555, CVE-2015-5556, CVE-2015-5557, CVE-2015-5558, CVE-2015-5559, CVE-2015-5560, CVE-2015-5561, CVE-2015-5562, CVE-2015-5563, CVE-2015-5564, CVE-2015-5565, AP SB15-19

Novell

How to fix: *Run the affected software's update mechanism, or go to the vendor's site to download the latest version and/or patches.*

Title: The latest release version of Firefox is not installed

Check ID: lua:com.iscanonline:def:5223

CVSS: 10.0

References: CVE-2015-4473, CVE-2015-4474, CVE-2015-4475, CVE-2015-4477, CVE-2015-4478, CVE-2015-4479, CVE-2015-4480, CVE-2015-4493, CVE-2015-4481, CVE-2015-4482, CVE-2015-4483, CVE-2015-4484, CVE-2011-4491, CVE-2015-4485, CVE-2015-4486, CVE-2015-4487, CVE-2015-4488, CVE-2015-4489, CVE-2015-4490, CVE-2015-4492, MFSA 2015-79, MFSA 2015-80, MFSA 2015-81, MFSA 2015-82, MFSA 2015-83, MFSA 2015-84, MFSA 2015-85, MFSA 2015-86, MFSA 2015-87, MFSA 2015-88, MFSA 2015-89, MFSA 2015-90, MFSA 2015-91, MFSA 2015-92

Title: Firefox 38.0 is not installed

Check ID: lua:com.iscanonline:def:5599
CVSS: 10.0
References: CVE-2015-2708, CVE-2015-2709, CVE-2015-0797, CVE-2015-2710, CVE-2015-2711, CVE-2015-2712, CVE-2015-2713, CVE-2015-2714, CVE-2015-2715, CVE-2015-2716, CVE-2015-2717, CVE-2015-2718, CVE-2011-3079, CVE-2015-2720, CVE-2015-0833, MFSA 2015-46, MFSA 2015-47, MFSA 2015-48, MFSA 2015-49, MFSA 2015-50, MFSA 2015-51, MFSA 2015-52, MFSA 2015-53, MFSA 2015-54, MFSA 2015-55, MFSA 2015-56, MFSA 2015-57, MFSA 2015-58

Title: Firefox 40.0 is not installed

Check ID: lua:com.iscanonline:def:6135

CVSS: 10.0

References: CVE-2015-4473, CVE-2015-4474, CVE-2015-4475, CVE-2015-4477, CVE-2015-4478, CVE-2015-4479, CVE-2015-4480, CVE-2015-4493, CVE-2015-4481, CVE-2015-4482, CVE-2015-4483, CVE-2015-4484, CVE-2011-4491, CVE-2015-4485, CVE-2015-4486, CVE-2015-4487, CVE-2015-4488, CVE-2015-4489, CVE-2015-4490, CVE-2015-4492, MFSA 2015-79, MFSA 2015-80, MFSA 2015-81, MFSA 2015-82, MFSA 2015-83, MFSA 2015-84, MFSA 2015-85, MFSA 2015-86, MFSA 2015-87, MFSA 2015-88, MFSA 2015-89, MFSA 2015-90, MFSA 2015-91, MFSA 2015-92

Title: Firefox 39.0 is not installed

Check ID: lua:com.iscanonline:def:6042

CVSS: 10.0

References: CVE-2015-2724, CVE-2015-2725, CVE-2015-2726, CVE-2015-2727, CVE-2015-2728, CVE-2015-2729, CVE-2015-2731, CVE-2015-2730, CVE-2015-2722, CVE-2015-2733, CVE-2015-2734, CVE-2015-2735, CVE-2011-2736, CVE-2015-2737, CVE-2015-2738, CVE-2015-2739, CVE-2015-2740, CVE-2015-2741, CVE-2015-2742, CVE-2015-2743, CVE-2015-4000, CVE-2015-2721, MFSA 2015-59, MFSA 2015-60, MFSA 2015-61, MFSA 2015-62, MFSA 2015-63, MFSA 2015-64, MFSA 2015-65, MFSA 2015-66, MFSA 2015-67, MFSA 2015-68, MFSA 2015-69, MFSA 2015-70, MFSA 2015-71

Mozilla

How to fix: *Run the affected software's update mechanism, or go to the vendor's site to download the latest version and/or patches.*

Title: Firefox 31.0 is not installed

Check ID: lua:com.iscanonline:def:5198

CVSS: 10.0

References: CVE-2014-1547, CVE-2014-1548, CVE-2014-1549, CVE-2014-1550, CVE-2014-1551, CVE-2014-1561, CVE-2014-1555, CVE-2014-1556, CVE-2014-1544, CVE-2014-1557, CVE-2014-1558, CVE-2014-1559, CVE-2014-1560, CVE-2014-1552, MFSA 2014-56, MFSA 2014-57, MFSA 2014-58, MFSA 2014-59, MFSA 2014-60, MFSA 2014-61, MFSA 2014-62, MFSA 2014-63, MFSA 2014-64, MFSA 2014-65, MFSA 2014-66

Title: Firefox 35.0 is not installed

Check ID: lua:com.iscanonline:def:5358

CVSS: 7.5

References: CVE-2014-8634, CVE-2014-8635, CVE-2014-8637, CVE-2014-8638, CVE-2014-8639, CVE-2014-8640, CVE-2014-8641, CVE-2014-8643, CVE-2014-8642, CVE-2014-8636, MFSA 2015-01, MFSA 2015-02, MFSA 2015-03, MFSA 2015-04, MFSA 2015-05, MFSA 2015-06, MFSA 2015-07, MFSA 2015-08, MFSA 2015-09

Title: Firefox 36.0 is not installed

Check ID: lua:com.iscanonline:def:5470

CVSS: 7.5

References: CVE-2015-0835, CVE-2015-0836, CVE-2015-0833, CVE-2015-0832, CVE-2015-0830, CVE-2015-0834, CVE-2015-0831, CVE-2015-0829, CVE-2015-0828, CVE-2015-0827, CVE-2015-0826, CVE-2015-0825, CVE-2015-0824, CVE-2015-0823, CVE-2015-0822, CVE-2015-0821, CVE-2015-0819, CVE-2015-0820, MFSA 2015-11, MFSA 2015-12, MFSA 2015-13, MFSA 2015-14, MFSA 2015-15, MFSA 2015-16, MFSA 2015-17, MFSA 2015-18, MFSA 2015-19, MFSA 2015-20, MFSA 2015-21, MFSA 2015-22, MFSA 2015-23, MFSA 2015-24, MFSA 2015-25, MFSA 2015-26, MFSA 2015-27

Title: Firefox 33.0 is not installed

Check ID: lua:com.iscanonline:def:5260

CVSS: 7.5

References: CVE-2014-1574, CVE-2014-1575, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1580, CVE-2014-1580, CVE-2014-1582, CVE-2014-1584, CVE-2014-1585, CVE-2014-1586, CVE-2014-1583, MFSA 2014-74, MFSA 2014-75, MFSA 2014-76, MFSA 2014-77, MFSA 2014-78, MFSA 2014-79, MFSA 2014-80, MFSA 2014-81, MFSA 2014-82

Title: Firefox 32.0 is not installed

Check ID: lua:com.iscanonline:def:5221

CVSS: 10.0

References: CVE-2014-1554, CVE-2014-1563, CVE-2014-1564, CVE-2014-1565, CVE-2014-1566, CVE-2014-1567, MFSA 2014-67, MFSA 2014-68, MFSA 2014-69, MFSA 2014-70, MFSA 2014-71, MFSA 2014-72

Title: Firefox 37.0 is not installed

Check ID: lua:com.iscanonline:def:5515

CVSS: 7.5

References: CVE-2015-0815, CVE-2015-0814, CVE-2015-0813, CVE-2015-0812, CVE-2015-0816, CVE-2015-0811, CVE-2015-0810, CVE-2015-0808, CVE-2015-0807, CVE-2015-0805, CVE-2015-0806, CVE-2015-0803, CVE-2015-0804, CVE-2015-0801, CVE-2015-0800, CVE-2012-2808, CVE-2015-0802, MFSA 2015-30, MFSA 2015-31, MFSA 2015-32, MFSA 2015-33, MFSA 2015-34, MFSA 2015-35, MFSA 2015-36, MFSA 2015-37, MFSA 2015-38, MFSA 2015-39, MFSA 2015-40, MFSA 2015-41, MFSA 2015-42

Title: Firefox 34.0 is not installed

Check ID: lua:com.iscanonline:def:5347

CVSS: 6.8

References: CVE-2014-1587, CVE-2014-1588, CVE-2014-1589, CVE-2014-1590, CVE-2014-1591, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-1595, CVE-2014-8632, CVE-2014-8631, MFSA 2014-83, MFSA 2014-84, MFSA 2014-85, MFSA 2014-86, MFSA 2014-87, MFSA 2014-88, MFSA 2014-89, MFSA 2014-90, MFSA 2014-91

Network Port Details

This section displays the open and listening TCP/IP ports on this system. Open ports indicate that a service is listening for external communication from a remote computer. Review the list of open ports to determine if they are absolutely necessary. Disable any unnecessary services to reduce the risk of compromise from malware or attackers. We recommend that you back up your system before making any changes. Your local IT administrator will be able to provide you with guidance on managing your network ports.

Result			
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49162	0.0.0.0:0	LISTENING
TCP	10.211.55.3:139	0.0.0.0:0	LISTENING
TCP	127.0.0.1:17600	0.0.0.0:0	LISTENING
TCP	127.0.0.1:17603	0.0.0.0:0	LISTENING
TCP	:::135	:::0	LISTENING
TCP	:::445	:::0	LISTENING
TCP	:::49152	:::0	LISTENING
TCP	:::49153	:::0	LISTENING
TCP	:::49154	:::0	LISTENING
TCP	:::49155	:::0	LISTENING
TCP	:::49156	:::0	LISTENING
TCP	:::49162	:::0	LISTENING