National Critical Information Infrastructure Protection Centre

CVE Report

1-30 March 2016

Vol. 3
No.5

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Application					
ABB					
Panel Builder 800 *Panel Builder is a user-friendly engineering tool to configure Panel 800 operator panels.*					
Gain Privileges	18-March-16	6	Untrusted search path vulnerability in ABB Panel Builder 800 5.1 allows local users to gain privileges via a Trojan horse DLL in the current working directory. **Reference:CVE-2016-2281**	https://ics-cert.us-cert.gov/advisories/ICSA-16-077-01	A-ABB-PANEL-40416/1
Adobe					
AIR;Air Sdk;Air Sdk & Compiler;Flash Player *The Adobe AIR runtime enables developers to package the same code into native applications and games for Windows and Mac OS desktops.* *AIR SDK & Compiler provides developers with a consistent and flexible development environment for the delivery of out-of-browser applications and games across devices and platforms (Windows, Mac, iOS, Android).*					

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service;Execute Code;Overflow;Memory Corruption	04-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2015-8820**	https://helpx.adobe.com/security/products/flash-player/apsb15-32.html	A-ADO-AIR-A-40416/2
Denial of Service;Execute Code;Overflow;Memory Corruption	04-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2015-8658**	https://helpx.adobe.com/security/products/flash-player/apsb15-32.html	A-ADO-AIR-A-40416/3

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service;Execute Code;Overflow;Memory Corruption	04-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2015-8657**	https://helpx.adobe.com/security/products/flash-player/apsb15-32.html	A-ADO-AIR-A-40416/4
Denial of Service;Execute Code;Overflow;Memory Corruption	04-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2015-8656**	https://helpx.adobe.com/security/products/flash-player/apsb15-32.html	A-ADO-AIR-A-40416/5
Denial of Service;Execute Code;Overflow;Memory	04-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on	https://helpx.adobe.com/security/products/flash-player/apsb1	A-ADO-AIR-A-40416/6

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Corruption			Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2015-8654**	5-32.html	
Denial of Service;Execute Code;Overflow;Memory Corruption	04-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2015-8652**	https://helpx.adobe.com/security/products/flash-player/apsb15-32.html	A-ADO-AIR-A-40416/7
Execute Code	04-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before	https://helpx.adobe.com/security/products/flash-player/apsb15-32.html	A-ADO-AIR-A-40416/8

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2015-8822**		
Execute Code	04-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2015-8821**	https://helpx.adobe.com/security/products/flash-player/apsb15-32.html	A-ADO-AIR-A-40416/9
Execute Code	04-March-16	9.3	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted	https://helpx.adobe.com/security/products/flash-player/apsb15-32.html	A-ADO-AIR-A-40416/10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			MPEG-4 data. **Reference:CVE -2015-8655**		
Execute Code	04-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2015-8653**	https://helpx.adobe.com/security/products/flash-player/apsb15-32.html	A-ADO-AIR-A-40416/11
Denial of Service;Execute Code;Overflow;Memory Corruption	12-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-1005**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/12

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service;Execute Code;Overflow;Memory Corruption	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-1002**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/13
Denial of Service;Execute Code;Overflow;Memory Corruption	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0992**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/14
Denial of Service;Execute Code;Overflow;Memory	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on	https://helpx.adobe.com/security/products/flash-player/apsb1	A-ADO-AIR-A-40416/15

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Corruption			Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0989**	6-08.html	
Denial of Service;Execute Code;Overflow;Memory Corruption	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0986**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/16
Denial of Service;Execute Code;Overflow;Memory Corruption	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/17

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0962**		
Denial of Service;Execute Code;Overflow;Memory Corruption	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0961**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/18
Denial of Service;Execute Code;Overflow;Memory Corruption	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/19

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0960**		
Execute Code	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-1000**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/20
Execute Code	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0999**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/21
Execute Code	12-March-	10	Adobe Flash Player before	https://helpx.	A-ADO-

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
	16		18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0998**	adobe.com/security/products/flash-player/apsb16-08.html	AIR-A-40416/22
Execute Code	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0997**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/23
Execute Code	12-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/24

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0996**		
Execute Code	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0995**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/25
Execute Code	12-March-16	9.3	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/26

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0994**		
Execute Code	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0991**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/27
Execute Code	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/28

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			MPEG-4 data. **Reference:CVE -2016-0990**		
Execute Code	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0988**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/29
Execute Code	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-0987**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/30
Execute Code; Overflow	12-March-16	10	Adobe Flash Player before 18.0.0.268 and 19.x and	https://helpx.adobe.com/s	A-ADO-AIR-A-

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data. **Reference:CVE -2016-1010**	ecurity/products/flash-player/apsb16-08.html	40416/31
Execute Code; Overflow	12-March-16	10	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE -2016-1001**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/32
Execute Code; Overflow	12-March-16	10	Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/33

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0963 and CVE-2016-1010. **Reference:CVE -2016-0993**		
Execute Code; Overflow	12-March-16	10	Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0993 and CVE-2016-1010. **Reference:CVE -2016-0963**	https://helpx.adobe.com/security/products/flash-player/apsb16-08.html	A-ADO-AIR-A-40416/34
Digital Editions *Adobe Digital Editions (ADE) to proof-read their books.*					
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	10	Adobe Digital Editions before 4.5.1 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via	https://helpx.adobe.com/security/products/Digital-Editions/apsb16-06.html	A-ADO-DIGIT-40416/35

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			unspecified vectors. **Reference:CVE -2016-0954**		
Apple					
Safari *Safari is a web browser developed by Apple based on the WebKit engine.*					
Gain Information	23-March-16	4.3	The Top Sites feature in Apple Safari before 9.1 mishandles cookie storage, which makes it easier for remote web servers to track users via unspecified vectors. **Reference:CVE -2016-1772**	https://support.apple.com/HT206171	A-APP-SAFAR-40416/36
Denial of Service	23-March-16	7.1	The Downloads feature in Apple Safari before 9.1 mishandles file expansion, which allows remote attackers to cause a denial of service via a crafted web site. **Reference:CVE -2016-1771**	https://support.apple.com/HT206171	A-APP-SAFAR-40416/37
Not Avialable	23-March-16	4.3	Apple Safari before 9.1 allows remote attackers to spoof the user interface via a web page that places text in a crafted context, leading to unintended use of that text within a Safari dialog. **Reference:CVE -2009-2197**	https://support.apple.com/HT206171	A-APP-SAFAR-40416/38
Software Update *Software Update is the easiest and quickest solution to check and update software installed on your computer.*					
Not Avialable	13-March-16	5	Apple Software Update before 2.2 on Windows does not use HTTPS, which makes it easier for	https://support.apple.com/kb/HT206091	A-APP-SOFTW-40416/39

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			man-in-the-middle attackers to spoof updates by modifying the client-server data stream. **Reference:CVE -2016-1731**		
Xcode *Xcode is an integrated development environment (IDE) containing a suite of software development tools developed by Apple for developing software for OS X and iOS.*					
Denial of Service; Overflow; Gain Privileges; Memory Corruption	23-March-16	4.6	otool in Apple Xcode before 7.3 allows local users to gain privileges or cause a denial of service (memory corruption and application crash) via unspecified vectors. **Reference:CVE -2016-1765**	https://support.apple.com/HT206172	A-APP-XCODE-40416/40
Autodesk					
Autodesk Backburner *Autodesk Backburner is a background rendering network system that allows animation scenes to be rendered by many computers working collectively on the same network*					
Denail of Service;Execute Code;Overflow	28-March-16	7.8	Stack-based buffer overflow in manager.exe in Backburner Manager in Autodesk Backburner 2016 2016.0.0.2150 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted command. NOTE: this is only a vulnerability in environments in which the administrator has not followed documentation that outlines the security risks of operating Backburner on untrusted networks. **Reference:CVE -2016-**	http://www.kb.cert.org/vuls/id/732760	A-AUT-AUTOD-40416/41

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			2344		
CA					
Single Sign-on *Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords.*					
Denial of Service;Gain Information	23-March-16	6.4	The non-Domino web agents in CA Single Sign-On (aka SSO, formerly SiteMinder) R6, R12.0 before SP3 CR13, R12.0J before SP3 CR1.2, and R12.5 before CR5 allow remote attackers to cause a denial of service (daemon crash) or obtain sensitive information via a crafted request. **Reference:CVE -2015-6854**	http://www.ca.com/us/support/ca-support-online/productcontent/recommended-reading/security notices/ca20160323-01-security-notice-for-ca-single-sign-on-web-agents.aspx	A-CA-SINGL-40416/42
Denial of Service;Gain Information	23-March-16	6.4	The Domino web agent in CA Single Sign-On (aka SSO, formerly SiteMinder) R6, R12.0 before SP3 CR13, R12.0J before SP3 CR1.2, R12.5 before CR5, R12.51 before CR4, and R12.52 before SP1 CR3 allows remote attackers to cause a denial of service (daemon crash) or obtain sensitive information via a crafted request. **Reference:CVE -2015-6853**	http://www.ca.com/us/support/ca-support-online/product-content/recommended-reading/security-notices/ca20160323-01-security-notice-for-ca-single-sign-on-web-agents.aspx	A-CA-SINGL-40416/43

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Cisco					
Cisco Policy Suite *Cisco Policy Suite for Mobile is a proven carrier-grade policy, charging, and subscriber data management solution.*					
Bypass;Gain Information	03-March-16	5	The password-management administration component in Cisco Policy Suite (CPS) 7.0.1.3, 7.0.2, 7.0.2-att, 7.0.3-att, 7.0.4-att, and 7.5.0 allows remote attackers to bypass intended RBAC restrictions and read unspecified data via unknown vectors, aka Bug ID CSCut85211. **Reference:CVE -2016-1357**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-psc	A-CIS-CISCO-40416/44
Firesight System Software *The Cisco FireSIGHT System combines the security of an industry-leading network intrusion protection system with the power to control access to your network based on detected applications, users, and URLs.*					
Cross Site Scripting	03-March-16	4.3	Cross-site scripting (XSS) vulnerability in the Device Management UI in the management interface in Cisco FireSIGHT System Software 6.1.0 allows remote attackers to inject arbitrary web script or HTML via a crafted value, aka Bug ID CSCuy41687. **Reference:CVE -2016-1355**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-FireSIGHT	A-CIS-FIRES-40416/45
Not Avialable	03-March-16	4.3	Cisco FireSIGHT System Software 6.1.0 does not use a constant-time algorithm for verifying credentials, which makes it easier for remote	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-FIRES-40416/46

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			attackers to enumerate valid usernames by measuring timing differences, aka Bug ID CSCuy41615. **Reference:CVE -2016-1356**	20160302-FireSIGHT1	
Prime Infrastructure *Cisco Prime Infrastructure simplifies the management of wireless and wired networks. It offers Day 0 and 1 provisioning, as well as Day N assurance from the branch to the data center.*					
Denial of Service; Overflow	03-March-16	5.5	Cisco Prime Infrastructure 2.2, 3.0, and 3.1(0.0) allows remote authenticated users to read arbitrary files or cause a denial of service via an XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, aka Bug ID CSCuw81497. **Reference:CVE -2016-1358**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-cpi	A-CIS-PRIME-40416/47
Execute Code	03-March-16	6.5	Cisco Prime Infrastructure 3.0 allows remote authenticated users to execute arbitrary code via a crafted HTTP request that is mishandled during viewing of a log file, aka Bug ID CSCuw81494. **Reference:CVE -2016-1359**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-cpi1	A-CIS-PRIME-40416/48
Prime Lan Management Solution *This LMS solution simplifies the configuration, administration, monitoring, and troubleshooting of Cisco networks.*					
Gain	11-March-	3	Cisco Prime LAN	http://tools.ci	A-CIS-

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Information	16		Management Solution (LMS) through 4.2.5 uses the same database decryption key across different customers' installations, which allows local users to obtain cleartext data by leveraging console connectivity, aka Bug ID CSCuw85390. **Reference:CVE -2016-1360**	sco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160310-prime-lms	PRIME-40416/49
Telepresence Video Communication Server Software *The Cisco TelePresence Video Communication Server (VCS) provides flexible and extensible video conferencing applications.*					
Denial of Service	11-March-16	8	Cisco TelePresence Video Communication Server (VCS) X8.5.1 and X8.5.2 allows remote authenticated users to cause a denial of service (VoIP outage) via a crafted SIP message, aka Bug ID CSCuu43026. **Reference:CVE -2016-1338**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-vcs	A-CIS-TELEP-40416/50
Unified Communications Domain Manager *Cisco Unified Communications Domain Manager (CUCDM) is the UC domain manager within Cisco Hosted Collaboration Solution (HCS). Cisco UCDM empowers service providers and large enterprises to manage their UC services and applications, and the various disparate network elements, from a single platform.*					
Cross Site Scripting	03-March-16	4.3	Cross-site scripting (XSS) vulnerability in Cisco Unified Communications Domain Manager (UCDM) 8.x before 8.1.1 allows remote attackers to inject arbitrary web script or HTML via crafted markup data, aka Bug ID	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-cucdm	A-CIS-UNIFI-40416/51

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			CSCud41176. **Reference:CVE -2016-1354**		
Cross Site Scripting	28-March-16	3.5	Cross-site scripting (XSS) vulnerability in Cisco Unified Communications Domain Manager (CDM) 8.1(1) allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCux80760. **Reference:CVE -2016-1314**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160328-ucdm	A-CIS-UNIFI-40416/52
Cogent Datahub					
Cogent Datahub *Cogent DataHub provides a multi-purpose nerve-center transforming process data into usable information.*					
Gain Privileges	29-March-16	7.2	Cogent DataHub before 7.3.10 allows local users to gain privileges by leveraging the user or guest role to modify a file. **Reference:CVE -2016-2288**	https://ics-cert.us-cert.gov/advisories/ICSA-16-084-01	A-COG-COGEN-40416/53
Dropbear Ssh Project					
Dropbear Ssh *Dropbear is a relatively small SSH server and client. It runs on a variety of POSIX-based platforms. Dropbear is open source software.*					
Bypass	22-March-16	5.5	CRLF injection vulnerability in Dropbear SSH before 2016.72 allows remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data. **Reference:CVE -2016-3116**	https://matt.ucc.asn.au/dropbear/CHANGES	A-DRO-DROPB-40416/54

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Dte Energy					
Insight *Insight is a leading provider of hardware, software, cloud solutions and IT services to business, government, education and healthcare clients.*					
Gain Information	11-March-16	4	The REST API in the DTE Energy Insight application before 1.7.8 for Android allows remote authenticated users to obtain unspecified customer information via a SQL expression in the filter parameter. **Reference:CVE -2016-1562**	http://technet.microsoft.com/en-us/security/bulletin/ms16-027	A-DTE-INSIG-40416/55
EDX					
Open Edx *Open edX is the open source platform that powers edX courses. All edX code is freely available to the developer community.*					
Gain Information	19-March-16	4.3	lms/templates/footer-edx-new.html in Open edX edx-platform before 2015-01-29 does not properly restrict links on the password-reset page, which allows user-assisted remote attackers to discover password-reset tokens by reading a referer log after a victim navigates from this page to a social-sharing site. **Reference:CVE -2015-2286**	https://open.edx.org/	A-EDX-OPEN -40416/56
EMC					
Documentum Xcp *EMC Documentum xCP User licenses a set of integrated components for case management and business process management applications.*					
Gain Information	09-March-16	4	EMC Documentum xCP 2.1 before patch 24 and	http://seclists.org/bugtraq/	A-EMC-DOCUM-

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			2.2 before patch 12 allows remote authenticated users to obtain sensitive user-account metadata via a members/xcp_member API call. **Reference:CVE -2016-0886**	2016/Mar/44	40416/57
Google					
Chrome *Google Chrome is a browser that combines a minimal design with sophisticated technology to make the web faster, safer, and easier.*					
Gain Information	05-March-16	5	The Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 49.0.2623.75, does not ignore a URL's path component in the case of a ServiceWorker fetch, which allows remote attackers to obtain sensitive information about visited web pages by reading CSP violation reports, related to FrameFetchContext.cpp and ResourceFetcher.cpp. **Reference:CVE -2016-2845**	http://googlechromereleases.blogspot.com/2016/03/stable-channel-update.html	A-GOO-CHROM-40416/58
Gain Information	05-March-16	4.3	The SkATan2_255 function in effects/gradients/SkSweepGradient.cpp in Skia, as used in Google Chrome before 49.0.2623.75, mishandles arctangent calculations, which allows remote attackers to obtain sensitive information via a crafted	http://googlechromereleases.blogspot.com/2016/03/stable-channel-update.html	A-GOO-CHROM-40416/59

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			web site. **Reference:CVE -2016-1637**		
Bypass	05-March-16	6.8	extensions/renderer/resources/platform_app.js in the Extensions subsystem in Google Chrome before 49.0.2623.75 does not properly restrict use of Web APIs, which allows remote attackers to bypass intended access restrictions via a crafted platform app. **Reference:CVE -2016-1638**	http://googlechromereleases.blogspot.com/2016/03/stable-channel-update.html	A-GOO-CHROM-40416/60
Bypass	05-March-16	7.5	The PendingScript::notifyFinished function in WebKit/Source/core/dom/PendingScript.cpp in Google Chrome before 49.0.2623.75 relies on memory-cache information about integrity-check occurrences instead of integrity-check successes, which allows remote attackers to bypass the Subresource Integrity (aka SRI) protection mechanism by triggering two loads of the same resource. **Reference:CVE -2016-1636**	http://googlechromereleases.blogspot.com/2016/03/stable-channel-update.html	A-GOO-CHROM-40416/61
Bypass	05-March-16	6.8	The Extensions subsystem in Google Chrome before 49.0.2623.75 does not properly maintain own properties, which allows	http://googlechromereleases.blogspot.com/2016/03/stable-channel-	A-GOO-CHROM-40416/62

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			remote attackers to bypass intended access restrictions via crafted JavaScript code that triggers an incorrect cast, related to extensions/renderer/v8_helpers.h and gin/converter.h. **Reference:CVE -2016-1632**	update.html	
Bypass	05-March-16	6.8	The PPB_Flash_MessageLoop_Impl::InternalRun function in content/renderer/pepper/ppb_flash_message_loop_impl.cc in the Pepper plugin in Google Chrome before 49.0.2623.75 mishandles nested message loops, which allows remote attackers to bypass the Same Origin Policy via a crafted web site. **Reference:CVE -2016-1631**	http://googlechromereleases.blogspot.com/2016/03/stable-channel-update.html	A-GOO-CHROM-40416/63
Bypass	05-March-16	6.8	The ContainerNode::parserRemoveChild function in WebKit/Source/core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 49.0.2623.75, mishandles widget updates, which makes it easier for remote attackers to bypass the Same Origin Policy via a crafted web site. **Reference:CVE -2016-1630**	https://codereview.chromium.org/1464223002	A-GOO-CHROM-40416/64

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service	05-March-16	9.3	WebKit/Source/core/layout/LayoutBlock.cpp in Blink, as used in Google Chrome before 49.0.2623.75, does not properly determine when anonymous block wrappers may exist, which allows remote attackers to cause a denial of service (incorrect cast and assertion failure) or possibly have unspecified other impact via crafted JavaScript code. **Reference:CVE -2016-2844**	https://bugs.chromium.org/p/chromium/issues/detail?id=546849	A-GOO-CHROM-40416/65
Denial of Service	05-March-16	10	Multiple unspecified vulnerabilities in Google Chrome before 49.0.2623.75 allow attackers to cause a denial of service or possibly have other impact via unknown vectors. **Reference:CVE -2016-1642**	http://googlechromereleases.blogspot.com/2016/03/stable-channel-update.html	A-GOO-CHROM-40416/66
Denial of Service	05-March-16	9.3	Use-after-free vulnerability in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an image download after a certain data structure is deleted, as demonstrated by a favicon.ico download.	https://codereview.chromium.org/1730363003	A-GOO-CHROM-40416/67

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference:CVE -2016-1641		
Denial of Service	05-March-16	10	Use-after-free vulnerability in browser/extensions/api/webrtc_audio_private/webrtc_audio_private_api.cc in the WebRTC Audio Private API implementation in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect reliance on the resource context pointer. **Reference:CVE -2016-1639**	http://googlechromereleases.blogspot.com/2016/03/stable-channel-update.html	A-GOO-CHROM-40416/68
Denial of Service	05-March-16	10	extensions/renderer/renderer_frame_observer_natives.cc in Google Chrome before 49.0.2623.75 does not properly consider object lifetimes and re-entrancy issues during OnDocumentElementCreated handling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors. **Reference:CVE -2016-1635**	http://googlechromereleases.blogspot.com/2016/03/stable-channel-update.html	A-GOO-CHROM-40416/69
Denial of Service	05-March-16	9.3	Use-after-free vulnerability in the StyleResolver::appendCSSStyleSheet function in WebKit/Source/core/css/resolver/StyleResolver.cpp	http://googlechromereleases.blogspot.com/2016/03/stable-channel-	A-GOO-CHROM-40416/70

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site that triggers Cascading Style Sheets (CSS) style invalidation during a certain subtree-removal action. **Reference:CVE -2016-1634**	update.html	
Denial of Service	05-March-16	10	Use-after-free vulnerability in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors. **Reference:CVE -2016-1633**	https://code.google.com/p/chromium/issues/detail?id=572537	A-GOO-CHROM-40416/71
Denial of Service	13-March-16	9.3	WebKit/Source/core/layout/LayoutObject.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly restrict relayout scheduling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted HTML document. **Reference:CVE -2016-1644**	https://codereview.chromium.org/1755543002	A-GOO-CHROM-40416/72
Denial of Service	13-March-16	9.3	The ImageInputType::ensurePrimaryContent function in	https://codereview.chromium.org/1732	A-GOO-CHROM-40416/73

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			WebKit/Source/core/html/forms/ImageInputType.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly maintain the user agent shadow DOM, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion." **Reference:CVE -2016-1643**	753004	
Denial of Service	29-March-16	9.3	The PageCaptureSaveAsMHTMLFunction::ReturnFailure function in browser/extensions/api/page_capture/page_capture_api.cc in Google Chrome before 49.0.2623.108 allows attackers to cause a denial of service or possibly have unspecified other impact by triggering an error in creating an MHTML document. **Reference:CVE -2016-1650**	http://google chromereleases.blogspot.com/2016/03/stable-channel-update_24.html	A-GOO-CHROM-40416/74
Denial of Service	29-March-16	9.3	Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or	http://google chromereleases.blogspot.com/2016/03/stable-channel-update_24.html	A-GOO-CHROM-40416/75

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			possibly have unspecified other impact via crafted JavaScript code. **Reference:CVE -2016-1648**		
Denial of Service	29-March-16	9.3	Use-after-free vulnerability in the RenderWidgetHostImpl::Destroy function in content/browser/renderer_host/render_widget_host_impl.cc in the Navigation implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors. **Reference:CVE -2016-1647**	http://google chromereleases.blogspot.com/2016/03/stable-channel-update_24.html	A-GOO-CHROM-40416/76
Denial of Service; Overflow	13-March-16	9.3	Multiple integer signedness errors in the opj_j2k_update_image_data function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 49.0.2623.87, allow remote attackers to cause a denial of service (incorrect cast and out-of-bounds write) or possibly have unspecified other impact via crafted JPEG 2000 data. **Reference:CVE -2016-1645**	http://www.zerodayinitiative.com/advisories/ZDI-16-197/	A-GOO-CHROM-40416/77
Denial of Service; Overflow	29-March-16	9.3	The Program::getUniformInternal function in Program.cpp in libANGLE, as used in Google Chrome	http://google chromereleases.blogspot.com/2016/03/stable-	A-GOO-CHROM-40416/78

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			before 49.0.2623.108, does not properly handle a certain data-type mismatch, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted shader stages. **Reference:CVE -2016-1649**	channel-update_24.html	
Denial of Service; Overflow	29-March-16	9.3	The Array.prototype.concat implementation in builtins.cc in Google V8, as used in Google Chrome before 49.0.2623.108, does not properly consider element data types, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted JavaScript code. **Reference:CVE -2016-1646**	http://googlechromereleases.blogspot.com/2016/03/stable-channel-update_24.html	A-GOO-CHROM-40416/79
Not Avialable	05-March-16	4.3	The Web Store inline-installer implementation in the Extensions UI in Google Chrome before 49.0.2623.75 does not block installations upon deletion of an installation frame, which makes it easier for remote attackers to trick a user into believing that an installation request originated from the user's next navigation target via a crafted web site.	http://googlechromereleases.blogspot.com/2016/03/stable-channel-update.html	A-GOO-CHROM-40416/80

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference:CVE -2016-1640		
Chrome;V8 *Google Chrome is a browser that combines a minimal design with sophisticated technology to make the web faster, safer, and easier.* *V8 is Google's open source high-performance JavaScript engine, written in C++ and used in Google Chrome, the open source browser from Google.*					
Denial of Service	05-March-16	10	Multiple unspecified vulnerabilities in Google V8 before 4.9.385.26, as used in Google Chrome before 49.0.2623.75, allow attackers to cause a denial of service or possibly have other impact via unknown vectors. **Reference:CVE -2016-2843**	http://google chromereleases.blogspot.com/2016/03/stable-channel-update.html	A-GOO-CHROM-40416/81
Graniteds					
Granite Data Services *Granite Data Services (GraniteDS) is a comprehensive development and integration solution for building Flex / JavaFX / Android / JavaEE RIA applications.*					
Denial of Service	25-March-16	5.5	The AMF framework in Granite Data Services 3.1.1-SNAPSHOT allows remote authenticated users to read arbitrary files, send TCP requests to intranet servers, or cause a denial of service via an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. **Reference:CVE -2016-2340**	http://www.kb.cert.org/vuls/id/279472	A-GRA-GRANI-40416/82
HP					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

National Critical Information Infrastructure Protection Centre

CVE Report

1-30 March 2016

Vol. 3 No.5

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Arcsight Enterprise Security Manager *ArcSight ESM software solution, an enterprise security management system for event correlation, compliance monitoring and compliance*					
Execute Code; Gain Privileges	16-March-16	4.3	HPE ArcSight ESM 5.x before 5.6, 6.0, 6.5.x before 6.5C SP1 Patch 2, and 6.8c before P1, and ArcSight ESM Express before 6.9.1, allows local users to gain privileges for command execution via unspecified vectors. **Reference:CVE -2016-1990**	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05048452	A-HP-ARCSI-40416/83
Not Available	16-March-16	6	HPE ArcSight ESM 5.x before 5.6, 6.0, 6.5.x before 6.5C SP1 Patch 2, and 6.8c before P1, and ArcSight ESM Express before 6.9.1, allows remote authenticated users to conduct unspecified "file download" attacks via unknown vectors. **Reference:CVE -2016-1991**	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05048452	A-HP-ARCSI-40416/84
Enterprise Security Manager;Enterprise Security Manager Express *Enterprise Security Manager delivers intelligent, fast, and accurate security and information (SIEM) and log management.; Enterprise security management software that combines event correlation and security analytics to identify and prioritize.*					
Gain Information	17-March-16	4	HPE ArcSight ESM before 6.8c, and ArcSight ESM Express before 6.9.1, allows remote authenticated users to obtain sensitive information via unspecified vectors. **Reference:CVE -2016-1992**	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05048753	A-HP-ENTER-40416/85

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

National Critical Information Infrastructure Protection Centre

CVE Report

1-30 March 2016

Vol. 3 No.5

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Network Automation *Automation software for Windows that allows you to automate business and IT processes via an easy to use drag-and-drop user interface.*					
Execute Code; Gain Information	14-March-16	10	HPE Network Automation 9.22 through 9.22.02 and 10.x before 10.00.02 allows remote attackers to execute arbitrary code or obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-1988. **Reference:CVE -2016-1989**	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05030906	A-HP-NETWO-40416/86
Execute Code; Gain Information	14-March-16	10	HPE Network Automation 9.22 through 9.22.02 and 10.x before 10.00.02 allows remote attackers to execute arbitrary code or obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-1989. **Reference:CVE -2016-1988**	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05030906	A-HP-NETWO-40416/87
Operations Orchestration;Operations Orchestration Content *IT process automation software for HP enables reduces operational costs, errors, downtime and risk of non-compliance while improving service*					
Execute Code	22-March-16	10	HPE Operations Orchestration 10.x before 10.51 and Operations Orchestration content before 1.7.0 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library.	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05050545	A-HP-OPERA-40416/88

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

National Critical Information Infrastructure Protection Centre

CVE Report

1-30 March 2016

Vol. 3 No.5

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference:CVE -2016-1997		
Service Manager *Service Manager provides an integrated platform for automating and adapting your organization's IT service management best practices.*					
Execute Code	22-March-16	10	HPE Service Manager (SM) 9.3x before 9.35 P4 and 9.4x before 9.41.P2 allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library. **Reference:CVE -2016-1998**	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05054565	A-HP-SERVI-40416/89
Support Assistant *HP Support Assistant is a one-stop solution for connected, contextual support for your PC and printers.*					
Bypass	19-March-16	10	HP Support Assistant before 8.1.52.1 allows remote attackers to bypass authentication via unspecified vectors. **Reference:CVE -2016-2245**	https://h20565.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c05031674	A-HP-SUPPO-40416/90
System Management Homepage *The System Management Homepage provides a consolidated view for single server management highlighting tightly integrated management functionalities .*					
Gain Information	18-March-16	3.6	HPE System Management Homepage before 7.5.4 allows local users to obtain sensitive information or modify data via unspecified vectors. **Reference:CVE -2016-1996**	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05045763	A-HP-SYSTE-40416/91

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

National Critical Information Infrastructure Protection Centre

CVE Report

1-30 March 2016

Vol. 3 No.5

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Gain Information	18-March-16	4	HPE System Management Homepage before 7.5.4 allows remote authenticated users to obtain sensitive information via unspecified vectors. **Reference:CVE -2016-1994**	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05045763	A-HP-SYSTE-40416/92
Gain Information	18-March-16	5.5	HPE System Management Homepage before 7.5.4 allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors. **Reference:CVE -2016-1993**	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05045763	A-HP-SYSTE-40416/93
Execute Code	18-March-16	10	HPE System Management Homepage before 7.5.4 allows remote attackers to execute arbitrary code via unspecified vectors. **Reference:CVE -2016-1995**	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05045763	A-HP-SYSTE-40416/94
IBM					
Business Process Manager *Business process management (BPM) is a systematic approach to making an organization's workflow more effective, more efficient and more capable of adapting to an ever-changing environment*					
Cross Site Scripting	03-March-16	3.5	Cross-site scripting (XSS) vulnerability in the document-list control implementation in IBM Business Process Manager (BPM) 8.0 through 8.0.1.3, 8.5.0 through 8.5.0.2, and 8.5.5 and 8.5.6 through 8.5.6.2 allows remote authenticated users to inject arbitrary web script	http://www-01.ibm.com/support/docview.wss?uid=swg21978058	A-IBM-BUSIN-40416/95

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			or HTML via a crafted URL. **Reference:CVE -2016-0227**		
Business Process Manager;Websphere Process Server *Business process management (BPM) is a systematic approach to making an organization's workflow more effective, more efficient and more capable of adapting to an ever-changing environment.; WebSphere Process Server is the runtime engine for artifacts produced in a business-driven development process.*					
Bypass	21-March-16	4	Business Space in IBM WebSphere Process Server 6.1.2.0 through 7.0.0.5 and Business Process Manager Advanced 7.5.x through 7.5.1.2, 8.0.x through 8.0.1.3, 8.5.0.x through 8.5.0.2, 8.5.5.x through 8.5.5.0, and 8.5.6.x through 8.5.6.2 allows remote authenticated users to bypass intended access restrictions and create an arbitrary page or space via unspecified vectors. **Reference:CVE -2015-7454**	http://www-01.ibm.com/support/docview.wss?uid=swg21972005	A-IBM-BUSIN-40416/96
Execute Code Sql Injection	12-March-16	6.5	SQL injection vulnerability in IBM Maximo Asset Management 7.1 through 7.1.1.13, 7.5.0 before 7.5.0.9 IFIX003, and 7.6.0 before 7.6.0.3 IFIX001; Maximo Asset Management 7.5.0 before 7.5.0.9 IFIX003, 7.5.1, and 7.6.0 before 7.6.0.3 IFIX001 for SmartCloud Control Desk; and Maximo Asset Management 7.1 through 7.1.1.13 and 7.2	http://www-01.ibm.com/support/docview.wss?uid=swg21974938	A-IBM-CHANG-40416/97

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			for Tivoli IT Asset Management for IT and certain other products allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. **Reference:CVE -2015-7448**		
Flashsystem V9000 Firmware *The FlashSystem V9000 includes data virtualization technology to help insulate hosts, hypervisors*					
Cross Site Scripting; Cross-site Request Forgery	12-March-16	6.8	Cross-site request forgery (CSRF) vulnerability in IBM Flash System V9000 7.4 before 7.4.1.4, 7.5 before 7.5.1.3, and 7.6 before 7.6.0.4 allows remote attackers to hijack the authentication of arbitrary users for requests that insert XSS sequences. **Reference:CVE -2015-7446**	http://www-01.ibm.com/support/docview.wss?uid=ssg1S1005570	A-IBM-FLASH-40416/98
Informix Dynamic Server *Informix Dynamic Server, also known as IDS, is an extensible Relational Database Management System originally developed by Informix Software Inc.*					
Gain Privileges	28-March-16	6.9	The client implementation in IBM Informix Dynamic Server 11.70.xCn on Windows does not properly restrict access to the (1) nsrd, (2) nsrexecd, and (3) portmap executable files, which allows local users to gain privileges via a Trojan horse file. **Reference:CVE -2016-**	http://www-01.ibm.com/support/docview.wss?uid=swg21978598	A-IBM-INFOR-40416/99

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			0226		
Infosphere Information Server *IBM InfoSphere Information Server is a market-leading data integration platform which includes a family of products that enable you to understand, cleanse, monitor, transform, and deliver data, as well as to collaborate to bridge the gap between business and IT.*					
Bypass	03-March-16	3.5	IBM InfoSphere Information Server 8.5 through FP3, 8.7 through FP2, 9.1 through 9.1.2.0, 11.3 through 11.3.1.2, and 11.5 allows remote authenticated users to bypass intended access restrictions via a modified cookie. **Reference:CVE -2015-7490**	http://www-01.ibm.com/support/docview.wss?uid=swg21975827	A-IBM-INFOS-40416/100
Maximo Asset Management *IBM Maximo Asset Management is an enterprise asset management (EAM) software solution product produced by IBM. It is a solution which is used to operate, maintain and dispose of enterprise assets.*					
Cross Site Scripting	13-March-16	3.5	Cross-site scripting (XSS) vulnerability in IBM Maximo Asset Management 7.1.1 through 7.1.1.3, 7.5.0 before 7.5.0.9 IFIX004, and 7.6.0 before 7.6.0.3 IFIX001 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference:CVE -2016-0262**	http://www-01.ibm.com/support/docview.wss?uid=swg21977828	A-IBM-MAXIM-40416/101
Tivoli Monitoring *IBM Tivoli Monitoring and Tivoli Composite Application Manager products help optimize IT infrastructure performance and availability.*					
Gain Privileges	11-March-16	9	The portal client in IBM Tivoli Monitoring (ITM)	http://www-01.ibm.com/s	A-IBM-TIVOL-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			6.2.2 through FP9, 6.2.3 through FP5, and 6.3.0 through FP6 allows remote authenticated users to gain privileges via unspecified vectors. **Reference:CVE -2015-7411**	upport/docview.wss?uid=swg21973559	40416/103
Tivoli Netview Access Services *Tivoli NetView Access Services act as mediator between a mainframe user and multiple applications sessions that are assigned to the user.*					
Gain Privileges	18-March-16	9	** DISPUTED ** IBM Tivoli NetView Access Services (NVAS) allows remote authenticated users to gain privileges by entering the ADM command and modifying a "page ID" field to the EMSPG2 transaction code. NOTE: the vendor's perspective is that configuration and use of available security controls in the NVAS product mitigates the reported vulnerability. **Reference:CVE -2014-9768**	http://www-01.ibm.com/support/docview.wss?uid=swg21973560	A-IBM-TIVOL-40416/104
Websphere Application Server *WebSphere Application Server (WAS) is a software product that performs the role of a web application server. More specifically, it is a software framework and middleware that hosts Java based web applications.*					
Cross Site Scripting	19-March-16	4.3	Cross-site scripting (XSS) vulnerability in the OpenID Connect (OIDC) client web application in IBM WebSphere Application Server (WAS) Liberty Profile 8.5.5 before 8.5.5.9 allows remote	http://www-01.ibm.com/support/docview.wss?uid=swg21978293	A-IBM-WEBSP-40416/105

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			attackers to inject arbitrary web script or HTML via a crafted URL. **Reference:CVE -2016-0283**		
Websphere Commerce *IBM WebSphere Commerce AKA WCS (WebSphere Commerce Suite) is a software platform framework for e-commerce, including marketing, sales, customer and order processing functionality in a tailorable, integrated package.*					
Denial of Service	13-March-16	4.3	IBM WebSphere Commerce 6.x through 6.0.0.11, 7.x through 7.0.0.9, and 8.x before 8.0.0.3 allows remote attackers to cause a denial of service (order-processing outage) via unspecified vectors. **Reference:CVE -2016-0208**	http://www-01.ibm.com/support/docview.wss?uid=swg21975774	A-IBM-WEBSP-40416/106
ISC					
Dhcp *Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.*					
Denial of Service	09-March-16	7.1	ISC DHCP 4.1.x before 4.1-ESV-R13 and 4.2.x and 4.3.x before 4.3.4 does not restrict the number of concurrent TCP sessions, which allows remote attackers to cause a denial of service (INSIST assertion failure or request-processing outage) by establishing many sessions. **Reference:CVE -2016-2774**	https://kb.isc.org/article/AA-01354	A-ISC-DHCP-40416/107
Microsoft					

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
.net Framework *.NET Framework. A comprehensive programming model for building any application, from mobile to web to desktop. Build powerful Windows, web, mobile apps and games using.*					
Bypass	09-March-16	10	Microsoft .NET Framework 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, and 4.6.1 mishandles signature validation for unspecified elements of XML documents, which allows remote attackers to spoof signatures via a modified document, aka ".NET XML Validation Security Feature Bypass." **Reference:CVE -2016-0132**	http://technet.microsoft.com/en-us/security/bulletin/ms16-035	A-MIC-.NET-40416/108
Edge *Microsoft Edge is a web browser developed by Microsoft and included in the company's Windows 10 operating systems.*					
Gain Information	09-March-16	2.6	Microsoft Edge mishandles the Referer policy, which allows remote attackers to obtain sensitive browser-history and request information via a crafted HTTPS web site, aka "Microsoft Edge Information Disclosure Vulnerability." **Reference:CVE -2016-0125**	http://technet.microsoft.com/en-us/security/bulletin/ms16-024	A-MIC-EDGE-40416/109
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability,"	http://technet.microsoft.com/en-us/security/bulletin/ms16-024	A-MIC-EDGE-40416/110

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			a different vulnerability than CVE-2016-0116, CVE-2016-0123, CVE-2016-0124, and CVE-2016-0129. **Reference:CVE -2016-0130**		
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0116, CVE-2016-0123, CVE-2016-0124, and CVE-2016-0130. **Reference:CVE -2016-0129**	http://technet.microsoft.com/en-us/security/bulletin/ms16-024	A-MIC-EDGE-40416/111
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0116, CVE-2016-0123, CVE-2016-0129, and CVE-2016-0130. **Reference:CVE -2016-0124**	http://technet.microsoft.com/en-us/security/bulletin/ms16-024	A-MIC-EDGE-40416/112
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka	http://technet.microsoft.com/en-us/security/bulletin/ms16-024	A-MIC-EDGE-40416/113

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			"Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0116, CVE-2016-0124, CVE-2016-0129, and CVE-2016-0130. **Reference:CVE -2016-0123**		
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0123, CVE-2016-0124, CVE-2016-0129, and CVE-2016-0130. **Reference:CVE -2016-0116**	http://technet.microsoft.com/en-us/security/bulletin/ms16-024	A-MIC-EDGE-40416/114
Edge;Internet Explorer *Microsoft Edge is a web browser developed by Microsoft and included in the company's Windows 10 operating systems. Internet Explorer is a series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems.*					
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-	http://technet.microsoft.com/en-us/security/bulletin/ms16-022	A-MIC-EDGE;-40416/115

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			0107, CVE-2016-0112, and CVE-2016-0113. **Reference:CVE -2016-0111**		
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 10 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." **Reference:CVE -2016-0110**	http://technet.microsoft.com/en-us/security/bulletin/ms16-021	A-MIC-EDGE;-40416/116
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0106, CVE-2016-0108, and CVE-2016-0114. **Reference:CVE -2016-0109**	http://technet.microsoft.com/en-us/security/bulletin/ms16-020	A-MIC-EDGE;-40416/117
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka	http://technet.microsoft.com/en-us/security/bulletin/ms16-022	A-MIC-EDGE;-40416/118

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			"Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0107, CVE-2016-0111, CVE-2016-0112, and CVE-2016-0113. **Reference:CVE -2016-0105**		
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0103, CVE-2016-0106, CVE-2016-0108, CVE-2016-0109, and CVE-2016-0114. **Reference:CVE -2016-0102**	http://technet.microsoft.com/en-us/security/bulletin/ms16-022	A-MIC-EDGE;-40416/119
Infopath *Microsoft InfoPath is a software application for designing, distributing, filling and submitting electronic forms containing structured data. Microsoft initially released InfoPath as part of Microsoft Office 2003 family.*					
Execute Code;Overflow;Memory Corruption	09-March-16	9.3	Microsoft InfoPath 2007 SP3, 2010 SP2, and 2013 SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference:CVE -2016-0021**	http://technet.microsoft.com/en-us/security/bulletin/ms16-029	A-MIC-INFOP-40416/120

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Internet Explorer *Internet Explorer is a series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems.*					
Denial of Service;Execute Code;Memory Corruption	09-March-16	9.3	The CAttrArray object implementation in Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (type confusion and memory corruption) via a malformed Cascading Style Sheets (CSS) token sequence in conjunction with modifications to HTML elements, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6048 and CVE-2015-6049. **Reference:CVE -2015-6184**	http://technet.microsoft.com/en-us/security/bulletin/ms16-028	A-MIC-INTER-40416/121
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0106, CVE-2016-0108, and CVE-2016-0109. **Reference:CVE -2016-0114**	http://technet.microsoft.com/en-us/security/bulletin/ms16-023	A-MIC-INTER-40416/122

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

National Critical Information Infrastructure Protection Centre

CVE Report

1-30 March 2016

Vol. 3
No.5

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0107, CVE-2016-0111, and CVE-2016-0112. **Reference:CVE -2016-0113**	http://technet.microsoft.com/en-us/security/bulletin/ms16-023	A-MIC-INTER-40416/123
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0107, CVE-2016-0111, and CVE-2016-0113. **Reference:CVE -2016-0112**	http://technet.microsoft.com/en-us/security/bulletin/ms16-023	A-MIC-INTER-40416/124
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability,"	http://technet.microsoft.com/en-us/security/bulletin/ms16-023	A-MIC-INTER-40416/125

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0106, CVE-2016-0109, and CVE-2016-0114. **Reference:CVE -2016-0108**		
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0105, CVE-2016-0111, CVE-2016-0112, and CVE-2016-0113. **Reference:CVE -2016-0107**	http://technet.microsoft.com/en-us/security/bulletin/ms16-023	A-MIC-INTER-40416/126
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0102, CVE-2016-0103, CVE-2016-0108, CVE-2016-0109, and CVE-2016-0114. **Reference:CVE -2016-0106**	http://technet.microsoft.com/en-us/security/bulletin/ms16-023	A-MIC-INTER-40416/127
Denial of	09-March-	7.6	Microsoft Internet	http://techne	A-MIC-

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Service;Execute Code;Overflow;Memory Corruption	16		Explorer 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability." **Reference:CVE -2016-0104**	t.microsoft.com/en-us/security/bulletin/ms16-023	INTER-40416/128
Denial of Service;Execute Code;Overflow;Memory Corruption	09-March-16	7.6	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0102, CVE-2016-0106, CVE-2016-0108, CVE-2016-0109, and CVE-2016-0114. **Reference:CVE -2016-0103**	http://technet.microsoft.com/en-us/security/bulletin/ms16-023	A-MIC-INTER-40416/129
Office *Web-based collaboration software application providing remote access to calendar, address book, email, and documents.*					
Gain Privileges; Bypass	09-March-16	7.2	Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, and 2016 does not properly sign an unspecified binary file, which allows local users to gain privileges via a Trojan horse file with a crafted signature, aka "Microsoft Office Security Feature Bypass Vulnerability." **Reference:CVE -2016-**	http://technet.microsoft.com/en-us/security/bulletin/ms16-029	A-MIC-OFFIC-40416/130

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			0057		
MIT					
Kerberos *Kerberos is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.*					
Denial of Service	25-March-16	3.5	The process_db_args function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in kadmind in MIT Kerberos 5 (aka krb5) through 1.13.4 and 1.14.x through 1.14.1 mishandles the DB argument, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted request to modify a principal. **Reference:CVE -2016-3119**	https://github.com/krb5/krb5/commit/08c642c09c38a9c6454ab43a9b53b2a89b9eef99	A-MIT-KERBE-40416/131
Mozilla					
Firefox *Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online.*					
Bypass;Gain Information	13-March-16	4.3	Mozilla Firefox before 45.0 does not properly restrict the availability of IFRAME Resource Timing API times, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via crafted JavaScript code that leverages	https://bugzilla.mozilla.org/show_bug.cgi?id=1246956	A-MOZ-FIREF-40416/132

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			history.back and performance.getEntries calls after restoring a browser session. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-7207. **Reference:CVE -2016-1967**		
Bypass;Gain Information	13-March-16	4.3	Mozilla Firefox before 45.0 allows remote attackers to bypass the Same Origin Policy and obtain sensitive information by reading a Content Security Policy (CSP) violation report that contains path information associated with an IFRAME element. **Reference:CVE -2016-1955**	https://bugzilla.mozilla.org/show_bug.cgi?id=1208946	A-MOZ-FIREF-40416/133
Denial of Service	13-March-16	6.8	Race condition in libvpx in Mozilla Firefox before 45.0 on Windows might allow remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors. **Reference:CVE -2016-1972**	https://bugzilla.mozilla.org/show_bug.cgi?id=1218124	A-MOZ-FIREF-40416/134
Denial of Service;Execute Code	13-March-16	6.8	Race condition in the GetStaticInstance function in the WebRTC implementation in Mozilla Firefox before 45.0 might allow remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via unspecified vectors.	https://bugzilla.mozilla.org/show_bug.cgi?id=1219339	A-MOZ-FIREF-40416/135

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference:CVE -2016-1973		
Denail of Service;Execute Code;Overflow	13-March-16	6.8	Integer underflow in Brotli, as used in Mozilla Firefox before 45.0, allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow) via crafted data with brotli compression. **Reference:CVE -2016-1968**	https://bugzilla.mozilla.org/show_bug.cgi?id=1246742	A-MOZ-FIREF-40416/136
Denial of Service;Execute Code;Overflow;Memory Corruption	13-March-16	6.8	The ServiceWorkerManager class in Mozilla Firefox before 45.0 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via unspecified use of the Clients API. **Reference:CVE -2016-1959**	https://bugzilla.mozilla.org/show_bug.cgi?id=1234949	A-MOZ-FIREF-40416/137
Denial of Service; Memory Corruption	13-March-16	7.1	Mozilla Firefox before 45.0 on Linux, when an Intel video driver is used, allows remote attackers to cause a denial of service (memory consumption or stack memory corruption) by triggering use of a WebGL shader. **Reference:CVE -2016-1956**	https://bugzilla.mozilla.org/show_bug.cgi?id=1199923	A-MOZ-FIREF-40416/138
Denial of Service; Overflow; Gain Privileges;	13-March-16	4.4	The FileReader class in Mozilla Firefox before 45.0 allows local users to gain privileges or cause a denial of service (memory	https://bugzilla.mozilla.org/show_bug.cgi?id=1238440	A-MOZ-FIREF-40416/139

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Memory Corruption			corruption) by changing a file during a FileReader API read operation. **Reference:CVE -2016-1963**		
Denial of Service; Overflow; Memory Corruption	13-March-16	6.8	The I420VideoFrame::CreateFrame function in the WebRTC implementation in Mozilla Firefox before 45.0 on Windows omits an unspecified status check, which might allow remote attackers to cause a denial of service (memory corruption) or possibly have other impact via unknown vectors. **Reference:CVE -2016-1971**	https://bugzilla.mozilla.org/show_bug.cgi?id=1217663	A-MOZ-FIREF-40416/140
Denial of Service; Overflow; Memory Corruption	13-March-16	6.8	Integer underflow in the srtp_unprotect function in the WebRTC implementation in Mozilla Firefox before 45.0 on Windows might allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors. **Reference:CVE -2016-1970**	https://bugzilla.mozilla.org/show_bug.cgi?id=1216837	A-MOZ-FIREF-40416/141
Firefox;Firefox Esr *Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online. Firefox ESR is intended for groups who deploy and maintain the desktop environment in large organizations such as schools, governments and businesses.*					
Execute Code	03-March-16	10	Use-after-free vulnerability in the mozilla::DataChannelConn	https://bugzilla.mozilla.org/show_bug.cg	A-MOZ-FIREF-40416/142

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			ection::Close function in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code by leveraging mishandling of WebRTC data-channel connections. **Reference:CVE -2016-1962**	i?id=1240760	
Not Avialable	13-March-16	4.3	Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 mishandle a navigation sequence that returns to the original page, which allows remote attackers to spoof the address bar via vectors involving the history.back method and the location.protocol property. **Reference:CVE -2016-1965**	https://bugzilla.mozilla.org/show_bug.cgi?id=1245264	A-MOZ-FIREF-40416/143
Not Avialable	13-March-16	4.3	browser/base/content/browser.js in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to spoof the address bar via a javascript: URL. **Reference:CVE -2016-1958**	http://hg.mozilla.org/releases/mozilla-release/rev/80ce3f1ffe03	A-MOZ-FIREF-40416/144
Firefox;Firefox Esr;Network Security Services *Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online. The Network Security Services are a set of open source libraries and tools used to implement and deploy applications for Internet security. Mozilla Firefox, a free Web browser. Firefox ESR is intended for groups who deploy and maintain the desktop environment in large organizations such as schools. governments and businesses.*					
Execute Code;	13-March-	6.8	Heap-based buffer	http://www.m	A-MOZ-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Overflow	16		overflow in Mozilla Network Security Services (NSS) before 3.19.2.3 and 3.20.x and 3.21.x before 3.21.1, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to execute arbitrary code via crafted ASN.1 data in an X.509 certificate. **Reference:CVE -2016-1950**	ozilla.org/security/announce/2016/mfsa2016-35.html	FIREF-40416/145
Firefox;Firefox Esr;Thunderbird *Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online. Firefox ESR is intended for groups who deploy and maintain the desktop environment in large organizations such as schools, governments and businesses. Thunderbird makes e-mailing safer, faster, and easier with features such as intelligent spam filters, a built-in RSS reader, and quick search.*					
Denial of Service;Gain Privileges	13-March-16	6.8	The nsCSPContext::SendReports function in dom/security/nsCSPContext.cpp in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 does not prevent use of a non-HTTP report-uri for a Content Security Policy (CSP) violation report, which allows remote attackers to cause a denial of service (data overwrite) or possibly gain privileges by specifying a URL of a local file. **Reference:CVE -2016-1954**	http://hg.mozilla.org/releases/mozilla-release/rev/5154bb929236	A-MOZ-FIREF-40416/146
Denial of Service;Execu	13-March-16	6.8	Integer underflow in the nsHtml5TreeBuilder class	https://bugzilla.mozilla.org	A-MOZ-FIREF-

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
te Code			in the HTML5 string parser in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) by leveraging mishandling of end tags, as demonstrated by incorrect SVG processing, aka ZDI-CAN-3545. **Reference:CVE -2016-1960**	/show_bug.cgi?id=1246014	40416/147
Denial of Service;Execute Code;Memory Corruption	13-March-16	6.8	The nsNPObjWrapper::GetNewOrUsed function in dom/plugins/base/nsJSNPRuntime.cpp in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code or cause a denial of service (invalid pointer dereference and memory corruption) via a crafted NPAPI plugin. **Reference:CVE -2016-1966**	http://hg.mozilla.org/releases/mozilla-release/rev/f0d2911a9a4e	A-MOZ-FIREF-40416/148
Denial of Service;Execute Code;Memory Corruption	13-March-16	6.8	Use-after-free vulnerability in the AtomicBaseIncDec function in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by leveraging mishandling of XML	https://bugzilla.mozilla.org/show_bug.cgi?id=1243335	A-MOZ-FIREF-40416/149

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			transformations. **Reference:CVE -2016-1964**		
Denail of Service;Execute Code;Overflow	13-March-16	6.8	The nsScannerString::AppendUnicodeTo function in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 does not verify that memory allocation succeeds, which allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via crafted Unicode data in an HTML, XML, or SVG document. **Reference:CVE -2016-1974**	http://www.mozilla.org/security/announce/2016/mfsa2016-34.html	A-MOZ-FIREF-40416/150
Denial of Service;Execute Code;Overflow;Memory Corruption	13-March-16	6.8	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 45.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to js/src/jit/arm/Assembler-arm.cpp, and unknown other vectors. **Reference:CVE -2016-1953**	http://www.mozilla.org/security/announce/2016/mfsa2016-16.html	A-MOZ-FIREF-40416/151
Denial of Service;Execute Code;Overflow;Memory Corruption	13-March-16	6.8	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allow remote attackers to cause a	http://www.mozilla.org/security/announce/2016/mfsa2016-16.html	A-MOZ-FIREF-40416/152

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors. **Reference:CVE -2016-1952**		
Denial of Service; Overflow	13-March-16	4.3	Memory leak in libstagefright in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to cause a denial of service (memory consumption) via an MPEG-4 file that triggers a delete operation on an array. **Reference:CVE -2016-1957**	https://bugzilla.mozilla.org/show_bug.cgi?id=1227052	A-MOZ-FIREF-40416/153
Execute Code	13-March-16	6.8	Use-after-free vulnerability in the nsHTMLDocument::SetBody function in dom/html/nsHTMLDocument.cpp in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code by leveraging mishandling of a root element, aka ZDI-CAN-3574. **Reference:CVE -2016-1961**	https://bugzilla.mozilla.org/show_bug.cgi?id=1249377	A-MOZ-FIREF-40416/154

Firefox;Network Security Services

Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online.

The Network Security Services are a set of open source libraries and tools used to implement and deploy applications for Internet security. Mozilla Firefox, a free Web browser. Firefox ESR is intended for groups who deploy and maintain the desktop environment in large organizations such as schools. governments and businesses.

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service	13-March-16	6.8	Use-after-free vulnerability in the PK11_ImportDERPrivateKeyInfoAndReturnKey function in Mozilla Network Security Services (NSS) before 3.21.1, as used in Mozilla Firefox before 45.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted key data with DER encoding. **Reference:CVE -2016-1979**	http://www.mozilla.org/security/announce/2016/mfsa2016-36.html	A-MOZ-FIREF-40416/155
Denial of Service	13-March-16	6.8	Use-after-free vulnerability in the ssl3_HandleECDHServerKeyExchange function in Mozilla Network Security Services (NSS) before 3.21, as used in Mozilla Firefox before 44.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact by making an SSL (1) DHE or (2) ECDHE handshake at a time of high memory consumption. **Reference:CVE -2016-1978**	http://www.mozilla.org/security/announce/2016/mfsa2016-15.html	A-MOZ-FIREF-40416/156

Mozilla;SIL

Firefox;FirefoxEsr/Graphite2

Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online

Firefox ESR is intended for groups who deploy and maintain the desktop environment in large organizations such as schools, governments and businesses.

Graphite is a project within SIL's scripts and software dev groups to provide cross-platform rendering for complex writing systems.

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service	13-March-16	6.8	The graphite2::FileFace::get_table_fn function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, does not initialize memory for an unspecified data structure, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted Graphite smart font. **Reference:CVE -2016-2795**	https://bugzilla.mozilla.org/show_bug.cgi?id=1243597	A-MOZ-FIREF-40416/157
Denial of Service	13-March-16	6.8	The graphite2::TtfUtil::GetTableInfo function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, does not initialize memory for an unspecified data structure, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted Graphite smart font. **Reference:CVE -2016-2790**	https://bugzilla.mozilla.org/show_bug.cgi?id=1243464	A-MOZ-FIREF-40416/158
Denial of Service;Execute Code;Overflow;Memory Corruption	13-March-16	6.8	The Machine::Code::decoder::analysis::set_ref function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers	https://bugzilla.mozilla.org/show_bug.cgi?id=1248876	A-MOZ-FIREF-40416/159

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			to execute arbitrary code or cause a denial of service (stack memory corruption) via a crafted Graphite smart font. **Reference:CVE -2016-1977**		
Denial of Service; Overflow	13-March-16	6.8	The graphite2::TtfUtil::CmapSubtable4NextCodepoint function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font. **Reference:CVE -2016-2802**	https://bugzilla.mozilla.org/show_bug.cgi?id=1248804	A-MOZ-FIREF-40416/160
Denial of Service; Overflow	13-March-16	6.8	The graphite2::TtfUtil::CmapSubtable12Lookup function in TtfUtil.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2797. **Reference:CVE -2016-2801**	https://bugzilla.mozilla.org/show_bug.cgi?id=1249920	A-MOZ-FIREF-40416/161
Denial of Service;	13-March-16	6.8	The graphite2::Slot::getAttr	https://bugzilla.mozilla.org	A-MOZ-FIREF-

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Overflow			function in Slot.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2792. **Reference:CVE -2016-2800**	/show_bug.cgi?id=1249338	40416/162
Denial of Service; Overflow	13-March-16	9.3	Heap-based buffer overflow in the graphite2::Slot::setAttr function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Graphite smart font. **Reference:CVE -2016-2799**	http://www.mozilla.org/security/announce/2016/mfsa2016-37.html	A-MOZ-FIREF-40416/163
Denial of Service; Overflow	13-March-16	6.8	The graphite2::GlyphCache::Loader::Loader function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact	https://bugzilla.mozilla.org/show_bug.cgi?id=1248805	A-MOZ-FIREF-40416/164

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			via a crafted Graphite smart font. **Reference:CVE -2016-2798**		
Denial of Service; Overflow	13-March-16	6.8	The graphite2::TtfUtil::CmapSubtable12Lookup function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2801. **Reference:CVE -2016-2797**	https://bugzilla.mozilla.org/show_bug.cgi?id=1243823	A-MOZ-FIREF-40416/165
Denial of Service; Overflow	13-March-16	6.8	Heap-based buffer overflow in the graphite2::vm::Machine::Code::Code function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Graphite smart font. **Reference:CVE -2016-2796**	https://bugzilla.mozilla.org/show_bug.cgi?id=1243816	A-MOZ-FIREF-40416/166
Denial of Service; Overflow	13-March-16	6.8	The graphite2::TtfUtil::CmapSubtable12NextCodepoint function in Graphite 2 before 1.3.6, as used in	https://bugzilla.mozilla.org/show_bug.cgi?id=1243526	A-MOZ-FIREF-40416/167

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font. **Reference:CVE -2016-2794**		
Denial of Service; Overflow	13-March-16	6.8	CachedCmap.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font. **Reference:CVE -2016-2793**	https://bugzilla.mozilla.org/show_bug.cgi?id=1243513	A-MOZ-FIREF-40416/168
Denial of Service; Overflow	13-March-16	6.8	The graphite2::Slot::getAttr function in Slot.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2800. **Reference:CVE -2016-2792**	https://bugzilla.mozilla.org/show_bug.cgi?id=1243482	A-MOZ-FIREF-40416/169

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service; Overflow	13-March-16	6.8	The graphite2::GlyphCache::glyph function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font. **Reference:CVE -2016-2791**	https://bugzilla.mozilla.org/show_bug.cgi?id=1243473	A-MOZ-FIREF-40416/170
Denial of Service; Overflow	13-March-16	6.8	The setAttr function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.6.1, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted Graphite smart font. **Reference:CVE -2016-1969**	https://bugzilla.mozilla.org/show_bug.cgi?id=1242322	A-MOZ-FIREF-40416/171
Mozilla;Webrtc Project					
Firefox/Webrtc *Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online.* *WebRTC is a free, open project that enables web browsers with Real-Time Communications (RTC) capabilities via simple JavaScript APIs.*					
Denial of Service	13-March-16	6.8	Use-after-free vulnerability in the DesktopDisplayDevice class in the WebRTC implementation in Mozilla Firefox before 45.0 on Windows might allow	https://bugzilla.mozilla.org/show_bug.cgi?id=1176340	A-MOZ-FIREF-40416/172

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors. **Reference:CVE -2016-1976**		
Denial of Service; Memory Corruption	13-March-16	6.8	Multiple race conditions in dom/media/systemservices/CamerasChild.cpp in the WebRTC implementation in Mozilla Firefox before 45.0 on Windows might allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors. **Reference:CVE -2016-1975**	http://hg.mozilla.org/releases/mozilla-release/rev/bafc86c12e63	A-MOZ-FIREF-40416/173
Netiq					
Self Service Password Reset *A self service password reset solution that allows an end user to self reset his domain password in windows active directory remotely from a web browser without calling the helpdesk is an essential requirement.*					
Cross Site Scripting	23-March-16	4.3	Cross-site scripting (XSS) vulnerability in NetIQ Self Service Password Reset (SSPR) 2.x and 3.x before 3.3.1 HF2 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference:CVE -2016-1599**	https://www.netiq.com/support/kb/doc.php?id=7017399	A-NET-SELF-40416/174
Novell					
Filr *Micro Focus Filr gives mobile professionals direct access to the home folders, shared network folders and personal files you've already secured.*					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Cross Site Scripting	18-March-16	4.3	Cross-site scripting (XSS) vulnerability in Novell Filr 1.2 before Hot Patch 4 allows remote attackers to inject arbitrary web script or HTML via a crafted URL. **Reference:CVE -2015-5968**	https://www.novell.com/support/kb/doc.php?id=7017078	A-NOV-FILR-40416/175
Openbsd					
Openssh *OpenSSH, also known as OpenBSD Secure Shell, is a suite of security-related network-level utilities based on the SSH protocol, which help to secure network.*					
Bypass	22-March-16	5.5	Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions. **Reference:CVE -2016-3115**	http://www.openssh.com/txt/x11fwd.adv	A-OPE-OPENS-40416/176
Openssl					
Openssl *OpenSSL is a software library to be used in applications that need to secure communications against eavesdropping or need to ascertain the identity of the party at the other end.*					
Gain Information	02-March-16	4.3	An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites	http://openssl.org/news/secadv/20160301.txt	A-OPE-OPENS-40416/177

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. **Reference:CVE -2016-0704**		
Gain Information	02-March-16	4.3	The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800. **Reference:CVE -2016-0703**	http://openssl.org/news/secadv/20160301.txt	A-OPE-OPENS-40416/178
Gain Information	03-March-16	1.9	The MOD_EXP_CTIME_COPY_FROM_PREBUF function in crypto/bn/bn_exp.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not properly consider cache-bank access times during	http://openssl.org/news/secadv/20160301.txt	A-OPE-OPENS-40416/179

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			modular exponentiation, which makes it easier for local users to discover RSA keys by running a crafted application on the same Intel Sandy Bridge CPU core as a victim and leveraging cache-bank conflicts, aka a "CacheBleed" attack. **Reference:CVE -2016-0702**		
Denial of Service	03-March-16	7.8	Memory leak in the SRP_VBASE_get_by_user implementation in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt, related to apps/s_server.c and crypto/srp/srp_vfy.c. **Reference:CVE -2016-0798**	http://openssl.org/news/secadv/20160301.txt	A-OPE-OPENS-40416/180
Denial of Service; Memory Corruption	03-March-16	10	Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed DSA private key. **Reference:CVE -2016-0705**	http://openssl.org/news/secadv/20160301.txt	A-OPE-OPENS-40416/181

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Denial of Service; Overflow	03-March-16	10	The doapr_outch function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not verify that a certain memory allocation succeeds, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-0799. **Reference:CVE -2016-2842**	http://openssl.org/news/secadv/20160301.txt	A-OPE-OPENS-40416/182
Denial of Service; Overflow	03-March-16	10	The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-2842. **Reference:CVE -2016-0799**	http://openssl.org/news/secadv/20160301.txt	A-OPE-OPENS-40416/183
Denial of Service; Overflow;	03-March-16	5	Multiple integer overflows in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before	https://git.openssl.org/?p=openssl.gi	A-OPE-OPENS-40416/184

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Memory Corruption			1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference) or possibly have unspecified other impact via a long digit string that is mishandled by the (1) BN_dec2bn or (2) BN_hex2bn function, related to crypto/bn/bn.h and crypto/bn/bn_print.c. **Reference:CVE -2016-0797**	t;a=commit;h=c175308407858afff3fc8c2e5e085d94d12edc7d	
Not Avialable	01-March-16	4.3	The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack. **Reference:CVE -2016-0800**	https://access.redhat.com/security/vulnerabilities/drown	A-OPE-OPENS-40416/185
Oracle					
Java *Java is a set of computer software and specifications developed by Sun Microsystems, later acquired by Oracle Corporation.*					
Not Avialable	24-March-16	9.3	Unspecified vulnerability in Oracle Java SE 7u97, 8u73, and 8u74 allows remote attackers to affect	http://www.oracle.com/technetwork/topics/security/a	A-ORA-JAVA-40416/186

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			confidentiality, integrity, and availability via unknown vectors related to the Hotspot sub-component. **Reference:CVE -2016-0636**	lert-cve-2016-0636-2949497.html	
Pcre					
Pcre *Perl Compatible Regular Expressions (PCRE) is a regular expression C library inspired by the regular expression capabilities in the Perl programming language.*					
Denial of Service; Overflow; Memory Corruption	28-March-16	7.5	pcre_jit_compile.c in PCRE 8.35 does not properly use table jumps to optimize nested alternatives, which allows remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via a crafted string, as demonstrated by packets encountered by Suricata during use of a regular expression in an Emerging Threats Open ruleset. **Reference:CVE -2014-9769**	https://redmine.openinfosecfoundation.org/issues/1693	A-PCR-PCRE-40416/187
Pcre;Pcre2 *Perl Compatible Regular Expressions (PCRE) is a regular expression C library inspired by the regular expression capabilities in the Perl programming language . PCRE2 (Perl Compatible Regular Expressions v2) is an open source library written in C that allows developers to add regular expression .*					
Denail of Service;Execute Code;Overflow	17-March-16	7.5	The compile_branch function in pcre_compile.c in PCRE 8.x before 8.39 and pcre2_compile.c in PCRE2 before 10.22 mishandles patterns containing an (*ACCEPT)	http://vcs.pcre.org/pcre?view=revision&revision=1631	A-PCR-PCRE;-40416/188

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			substring in conjunction with nested parentheses, which allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow) via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, aka ZDI-CAN-3542. **Reference:CVE -2016-3191**		
Phpmyadmin					
Phpmyadmin *phpMyAdmin is a free and open source tool written in PHP intended to handle the administration of MySQL or MariaDB with the use of a web browser.*					
Gain Information	01-March-16	5.8	The checkHTTP function in libraries/Config.class.php in phpMyAdmin 4.5.x before 4.5.5.1 does not verify X.509 certificates from api.github.com SSL servers, which allows man-in-the-middle attackers to spoof these servers and obtain sensitive information via a crafted certificate. **Reference:CVE -2016-2562**	https://www.phpmyadmin.net/security/PMASA-2016-13/	A-PHP-PHPMY-40416/189
Cross Site Scripting	01-March-16	3.5	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.4.x before 4.4.15.5 and 4.5.x before 4.5.5.1 allow remote authenticated users to inject arbitrary web script	https://www.phpmyadmin.net/security/PMASA-2016-12/	A-PHP-PHPMY-40416/190

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			or HTML via (1) normalization.php or (2) js/normalization.js in the database normalization page, (3) templates/database/structure/sortable_header.phtml in the database structure page, or (4) the pos parameter to db_central_columns.php in the central columns page. **Reference:CVE -2016-2561**		
Cross Site Scripting	01-March-16	4.3	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.15, 4.4.x before 4.4.15.5, and 4.5.x before 4.5.5.1 allow remote attackers to inject arbitrary web script or HTML via (1) a crafted Host HTTP header, related to libraries/Config.class.php; (2) crafted JSON data, related to file_echo.php; (3) a crafted SQL query, related to js/functions.js; (4) the initial parameter to libraries/server_privileges.lib.php in the user accounts page; or (5) the it parameter to libraries/controllers/TableSearchController.class.php in the zoom search page. **Reference:CVE -2016-2560**	https://github.com/phpmyadmin/phpmyadmin/commit/38fa1191049ac0c626a6684eea52068dfbbb5078	A-PHP-PHPMY-40416/191

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Cross Site Scripting	01-March-16	3.5	Cross-site scripting (XSS) vulnerability in the format function in libraries/sql-parser/src/Utils/Error.php in the SQL parser in phpMyAdmin 4.5.x before 4.5.5.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted query. **Reference:CVE -2016-2559**	https://www.phpmyadmin.net/security/PMASA-2016-10/	A-PHP-PHPMY-40416/192
Samba					
Samba *Samba is a re-implementation of the SMB/CIFS networking protocol, it facilitates file and printer sharing among Linux and Windows systems as an alternative to NFS.*					
Denial of Service; Overflow; Gain Information	13-March-16	4.9	The internal DNS server in Samba 4.x before 4.1.23, 4.2.x before 4.2.9, 4.3.x before 4.3.6, and 4.4.x before 4.4.0rc4, when an AD DC is configured, allows remote authenticated users to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from process memory by uploading a crafted DNS TXT record. **Reference:CVE -2016-0771**	https://bugzilla.samba.org/show_bug.cgi?id=11128	A-SAM-SAMBA-40416/193
Not Avialable	13-March-16	4	The SMB1 implementation in smbd in Samba 3.x and 4.x before 4.1.23, 4.2.x before 4.2.9, 4.3.x before 4.3.6, and 4.4.x before 4.4.0rc4 allows remote authenticated users to modify arbitrary ACLs by using a UNIX SMB1 call to	https://bugzilla.samba.org/show_bug.cgi?id=11648	A-SAM-SAMBA-40416/194

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			create a symlink, and then using a non-UNIX SMB1 call to write to the ACL content. **Reference:CVE -2015-7560**		
Symantec					
Endpoint Protection Manager *Symantec Endpoint Protection is a client-server solution that protects laptops,desktops, Windows and Mac computers, and servers in your network.*					
Execute Code	18-March-16	9.3	The SysPlant.sys driver in the Application and Device Control (ADC) component in the client in Symantec Endpoint Protection (SEP) 12.1 before RU6-MP4 allows remote attackers to execute arbitrary code via a crafted HTML document, related to "RWX Permissions." **Reference:CVE -2015-8154**	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160317_00	A-SYM-ENDPO-40416/195
Execute Code; Cross-site Request Forgery	18-March-16	8.5	Cross-site request forgery (CSRF) vulnerability in Symantec Endpoint Protection Manager (SEPM) 12.1 before RU6-MP4 allows remote authenticated users to hijack the authentication of administrators for requests that execute arbitrary code by adding lines to a logging script. **Reference:CVE -2015-8152**	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160317_00	A-SYM-ENDPO-40416/196
Execute Code Sql Injection	18-March-16	8.3	SQL injection vulnerability in Symantec Endpoint Protection Manager (SEPM) 12.1 before RU6-	http://www.symantec.com/security_response/securit	A-SYM-ENDPO-40416/197

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			MP4 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. **Reference:CVE -2015-8153**	yupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160317_00	
Vmware					
Vrealize Automation *VMware vRealize Business IT financial management features give you transparency and control over IT costs, services and quality.*					
Cross Site Scripting	16-March-16	3.5	Cross-site scripting (XSS) vulnerability in VMware vRealize Automation 6.x before 6.2.4 on Linux allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference:CVE -2015-2344**	http://www.vmware.com/security/advisories/VMSA-2016-0003.html	A-VMW-VREAL-40416/198
Cross Site Scripting	16-March-16	3.5	Cross-site scripting (XSS) vulnerability in VMware vRealize Business Advanced and Enterprise 8.x before 8.2.5 on Linux allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference:CVE -2016-2075**	http://www.vmware.com/security/advisories/VMSA-2016-0003.html	A-VMW-VREAL-40416/199
Wp Favorite Posts Project					
Wp Favorite Posts *Allows visitors to add favorite posts. This plugin use cookies for saving data so unregistered users can favorite a post.*					
Cross Site Scripting	25-March-16	4.3	Cross-site scripting (XSS) vulnerability in the WP	https://wordpress.org/plugi	A-WP -WP FA-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Favorite Posts plugin before 1.6.6 for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference:CVE -2016-1160**	ns/wp-favorite-posts/changelog/	40416/200
Operating System					
Apple					
Apple Tv;Iphone Os;Mac Os X;Watchos *Apple TV is a digital media player and a microconsole developed and sold by Apple Inc. iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.* *OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc. It is designed to run on Macintosh computer.* *watchos is the mobile operating system of the Apple Watch, developed by Apple Inc.*					
Gain Information	23-March-16	4.3	IOHIDFamily in Apple iOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows attackers to obtain sensitive kernel memory-layout information via a crafted app. **Reference:CVE -2016-1748**	https://support.apple.com/HT205641	OS-APP-APPLE-40416/201
Denial of Service	23-March-16	9.3	The kernel in Apple iOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows attackers to cause a denial of service via a crafted app. **Reference:CVE -2016-1752**	https://support.apple.com/HT206169	OS-APP-APPLE-40416/202
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	9.3	TrueTypeScaler in Apple iOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows remote attackers to execute	https://support.apple.com/HT205641	OS-APP-APPLE-40416/203

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			arbitrary code or cause a denial of service (memory corruption) via a crafted font file. **Reference:CVE -2016-1775**		
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	9.3	The kernel in Apple iOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1754. **Reference:CVE -2016-1755**	https://support.apple.com/HT206169	OS-APP-APPLE-40416/204
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	9.3	The kernel in Apple iOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1755. **Reference:CVE -2016-1754**	https://support.apple.com/HT206169	OS-APP-APPLE-40416/205
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	9.3	FontParser in Apple iOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted	https://support.apple.com/HT206169	OS-APP-APPLE-40416/206

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			PDF document. **Reference:CVE -2016-1740**		
Execute Code	23-March-16	9.3	Use-after-free vulnerability in the kernel in Apple iOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allows attackers to execute arbitrary code in a privileged context via a crafted app. **Reference:CVE -2016-1750**	https://support.apple.com/HT206169	OS-APP-APPLE-40416/207
Execute Code; Overflow	23-March-16	9.3	Multiple integer overflows in the kernel in Apple iOS before 9.3, OS X before 10.11.4, tvOS before 9.2, and watchOS before 2.2 allow attackers to execute arbitrary code in a privileged context via a crafted app. **Reference:CVE -2016-1753**	https://support.apple.com/HT206169	OS-APP-APPLE-40416/208
Execute Code; Bypass	23-March-16	9.3	The kernel in Apple iOS before 9.3, tvOS before 9.2, and watchOS before 2.2 does not properly restrict the execute permission, which allows attackers to bypass a code-signing protection mechanism via a crafted app. **Reference:CVE -2016-1751**	https://support.apple.com/HT206166	OS-APP-APPLE-40416/209

Iphone Os

iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.

OS X is a series of Unix-based graphical interface operating systems (OS) developed and

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
marketed by Apple Inc. It is designed to run on Macintosh computer. watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.					
Gain Information	23-March-16	4.3	WebKit in Apple iOS before 9.3 does not prevent hidden web views from reading orientation and motion data, which allows remote attackers to obtain sensitive information about a device's physical environment via a crafted web site. **Reference:CVE -2016-1780**	https://support.apple.com/HT206166	OS-APP-IPHON-40416/210
Gain Information	23-March-16	3.5	Messages in Apple iOS before 9.3 does not ensure that an auto-fill action applies to the intended message thread, which allows remote authenticated users to obtain sensitive information by providing a crafted sms: URL and reading a thread. **Reference:CVE -2016-1763**	https://support.apple.com/HT206166	OS-APP-IPHON-40416/211
Bypass	29-March-16	2.1	The XPC Services API in LaunchServices in Apple iOS before 9.3 allows attackers to bypass intended event-handler restrictions and modify an arbitrary app's events via a crafted app. **Reference:CVE -2016-1760**	https://support.apple.com/HT206166	OS-APP-IPHON-40416/212
Not Avialable	23-March-16	5	The Profiles component in Apple iOS before 9.3 does not properly validate certificates, which allows attackers to spoof an	https://support.apple.com/HT206166	OS-APP-IPHON-40416/213

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			MDM profile trust relationship via unspecified vectors. **Reference:CVE -2016-1766**		
Iphone Os;Mac Os X *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.* *OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc. It is designed to run on Macintosh computer.*					
Denial of Service;Execute Code	23-March-16	9.3	The kernel in Apple iOS before 9.3 and OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. **Reference:CVE -2016-1756**	https://support.apple.com/HT206167	OS-APP-IPHON-40416/214
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	7.2	AppleUSBNetworking in Apple iOS before 9.3 and OS X before 10.11.4 allows physically proximate attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted USB device. **Reference:CVE -2016-1734**	https://support.apple.com/HT206167	OS-APP-IPHON-40416/215
Denial of Service; Overflow; Gain Information	23-March-16	4.3	The kernel in Apple iOS before 9.3 and OS X before 10.11.4 allows attackers to obtain sensitive memory-layout information or cause a denial of service (out-of-bounds read) via a crafted	https://support.apple.com/HT206167	OS-APP-IPHON-40416/216

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			app. **Reference:CVE -2016-1758**		
Execute Code	23-March-16	9.3	Race condition in the kernel in Apple iOS before 9.3 and OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context via a crafted app. **Reference:CVE -2016-1757**	https://support.apple.com/HT206167	OS-APP-IPHON-40416/217
Iphone Os;Mac Os X;Watchos *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.* *OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc. It is designed to run on Macintosh computer.* *watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.*					
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	10	libxml2 in Apple iOS before 9.3, OS X before 10.11.4, and watchOS before 2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document. **Reference:CVE -2016-1761**	https://support.apple.com/HT206166	OS-APP-IPHON-40416/218
Not Avialable	23-March-16	2.6	Messages in Apple iOS before 9.3, OS X before 10.11.4, and watchOS before 2.2 does not properly implement a cryptographic protection mechanism, which allows remote attackers to read message attachments via vectors related to duplicate messages. **Reference:CVE -2016-1788**	https://support.apple.com/HT206168	OS-APP-IPHON-40416/219

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Mac Os X *OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc. It is designed to run on Macintosh computer.*					
Gain Information	23-March-16	4.3	The Content Security Policy (CSP) implementation in Messages in Apple OS X before 10.11.4 allows remote attackers to obtain sensitive information via a javascript: URL. **Reference:CVE -2016-1764**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/220
Bypass	23-March-16	4.3	The Reminders component in Apple OS X before 10.11.4 allows attackers to bypass an intended user-confirmation requirement and trigger a dialing action via a tel: URL. **Reference:CVE -2016-1770**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/221
Bypass	23-March-16	7.2	dyld in Apple OS X before 10.11.4 allows attackers to bypass a code-signing protection mechanism via a modified app. **Reference:CVE -2016-1738**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/222
Denial of Service	23-March-16	2.1	IOFireWireFamily in Apple OS X before 10.11.4 allows local users to cause a denial of service (NULL pointer dereference) via unspecified vectors. **Reference:CVE -2016-1745**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/223
Denial of Service;Execu	23-March-16	9.3	IOGraphics in Apple OS X before 10.11.4 allows	https://support.apple.com/	OS-APP-MAC O-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
te Code;Memory Corruption			attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1746. **Reference:CVE -2016-1747**	HT206167	40416/224
Denial of Service;Execute Code;Memory Corruption	23-March-16	9.3	IOGraphics in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1747. **Reference:CVE -2016-1746**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/225
Denial of Service;Execute Code;Memory Corruption	23-March-16	9.3	AppleRAID in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference:CVE -2016-1733**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/226
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	6.8	QuickTime in Apple OS X before 10.11.4 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Photoshop file. **Reference:CVE -2016-1769**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/227
Denial of Service;Execu	23-March-16	6.8	QuickTime in Apple OS X before 10.11.4 allows	https://support.apple.com/	OS-APP-MAC O-

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
te Code;Overflow;Memory Corruption			remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted FlashPix image, a different vulnerability than CVE-2016-1767. **Reference:CVE -2016-1768**	HT206167	40416/228
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	6.8	QuickTime in Apple OS X before 10.11.4 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted FlashPix image, a different vulnerability than CVE-2016-1768. **Reference:CVE -2016-1767**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/229
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	9.3	The kernel in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference:CVE -2016-1759**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/230
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	9.3	IOUSBFamily in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference:CVE -2016-1749**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/231
Denial of Service;Execute	23-March-16	9.3	The Intel driver in the Graphics Drivers subsystem in Apple OS X	https://support.apple.com/HT206167	OS-APP-MAC O-40416/232

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Code;Overflow;Memory Corruption			before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1743. **Reference:CVE -2016-1744**		
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	9.3	The Intel driver in the Graphics Drivers subsystem in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1744. **Reference:CVE -2016-1743**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/233
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	10	The NVIDIA driver in the Graphics Drivers subsystem in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference:CVE -2016-1741**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/234
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	6.8	Carbon in Apple OS X before 10.11.4 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a	https://support.apple.com/HT206167	OS-APP-MAC O-40416/235

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			crafted .dfont file. **Reference:CVE -2016-1737**		
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	9.3	Bluetooth in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1735. **Reference:CVE -2016-1736**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/236
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	9.3	Bluetooth in Apple OS X before 10.11.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-1736. **Reference:CVE -2016-1735**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/237
Denial of Service; Overflow; Gain Information	23-March-16	2.1	AppleRAID in Apple OS X before 10.11.4 allows local users to obtain sensitive kernel memory-layout information or cause a denial of service (out-of-bounds read) via unspecified vectors. **Reference:CVE -2016-1732**	https://support.apple.com/HT206167	OS-APP-MAC O-40416/238
Not Avialable	23-March-16	2.1	The code-signing subsystem in Apple OS X before 10.11.4 does not properly verify file ownership, which allows local users to determine	https://support.apple.com/HT206167	OS-APP-MAC O-40416/239

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			the existence of arbitrary files via unspecified vectors. **Reference:CVE -2016-1773**		
Mac Os X Server *A server operating system version of the Mac OS X operating system for Apple computers.*					
Gain Information	23-March-16	5	Wiki Server in Apple OS X Server before 5.1 allows remote attackers to obtain sensitive information from Wiki pages via unspecified vectors. **Reference:CVE -2016-1787**	https://support.apple.com/HT206173	OS-APP-MAC O-40416/240
Gain Information	23-March-16	5	Web Server in Apple OS X Server before 5.1 does not properly restrict access to .DS_Store and .htaccess files, which allows remote attackers to obtain sensitive configuration information via an HTTP request. **Reference:CVE -2016-1776**	https://support.apple.com/HT206173	OS-APP-MAC O-40416/241
Gain Information	23-March-16	5	The Time Machine server in Server App in Apple OS X Server before 5.1 does not notify the user about ignored permissions during a backup, which makes it easier for remote attackers to obtain sensitive information in opportunistic circumstances by reading backup data that lacks intended restrictions. **Reference:CVE -2016-1774**	https://support.apple.com/HT206173	OS-APP-MAC O-40416/242

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Not Avialable	23-March-16	5	Web Server in Apple OS X Server before 5.1 supports the RC4 algorithm, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors. **Reference:CVE -2016-1777**	https://support.apple.com/HT206173	OS-APP-MAC O-40416/243
Cisco					
Asa 5500 Csc-ssm Firmware *The Cisco ASA 5500 Series Content Security and Control Security Services Module (CSC-SSM) delivers industry-leading threat protection and content control.*					
Denial of Service; Overflow	09-March-16	7.8	The HTTPS inspection engine in the Content Security and Control Security Services Module (CSC-SSM) 6.6 before 6.6.1164.0 for Cisco ASA 5500 devices allows remote attackers to cause a denial of service (memory consumption or device reload) via a flood of HTTPS packets, aka Bug ID CSCue76147. **Reference:CVE -2016-1312**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-csc	OS-CIS-ASA 5-40416/244
Dpc2203 Cable Modem Firmware *The Cisco Model DPC2203 Cable Modem (DPC2203) is a high-speed cable modem with an embedded media terminal adapter (EMTA).*					
Execute Code; Overflow	09-March-16	10	Buffer overflow in the web server on Cisco DPC2203 and EPC2203 devices with firmware r1_customer_image allows remote attackers to execute arbitrary code via a crafted HTTP request,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-cmre	OS-CIS-DPC22-40416/245

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			aka Bug ID CSCuv05935. **Reference:CVE -2016-1327**		
Dpc3939 Wireless Residential Voice Gateway Firmware *The Cisco Model DPC3939 DOCSIS 3.0 16x4 Wireless Residential Voice Gateway is a high-performance home gateway.*					
Gain Information	09-March-16	7.8	The administration interface on Cisco DPC3939B and DPC3941 devices allows remote attackers to obtain sensitive information via a crafted HTTP request, aka Bug ID CSCus49506. **Reference:CVE -2016-1325**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-rgid	OS-CIS-DPC39-40416/246
IOS *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.*					
Denial of Service	24-March-16	7.8	The Wide Area Application Services (WAAS) Express implementation in Cisco IOS 15.1 through 15.5 allows remote attackers to cause a denial of service (device reload) via a crafted TCP segment, aka Bug ID CSCuq59708. **Reference:CVE -2016-1347**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-l4f	OS-CIS-IOS-40416/247
Ios Xr *IOS XR is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), used on their high-end carrier-grade routers such as the CRS series, 12000 series, and ASR9000 series.*					
Denial of Service	11-March-16	4.6	Cisco IOS XR through 4.3.2 on Gigabit Switch Router (GSR) 12000 devices does not properly check for a Bidirectional Forwarding Detection	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	OS-CIS-IOS X-40416/248

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			(BFD) header in a UDP packet, which allows remote attackers to cause a denial of service (line-card restart) via a crafted packet, aka Bug ID CSCuw56900. **Reference:CVE -2016-1361**	20160311-gsr	
Denial of Service	24-March-16	6.8	The SCP and SFTP modules in Cisco IOS XR 5.0.0 through 5.2.5 on Network Convergence System 6000 devices use weak permissions for system files, which allows remote authenticated users to cause a denial of service (overwrite) via unspecified vectors, aka Bug ID CSCuw75848. **Reference:CVE -2016-1366**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-ncs	OS-CIS-IOS X-40416/249
IOS;Ios Xe *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.* *Cisco IOS XE software provides a modular structure that significantly enhances software quality and performance by separating the data plane and control plan.*					
Denial of Service	25-March-16	7.8	Cisco IOS 15.3 and 15.4, Cisco IOS XE 3.8 through 3.11, and Cisco Unified Communications Manager allow remote attackers to cause a denial of service (device reload) via malformed SIP messages, aka Bug ID CSCuj23293. **Reference:CVE -2016-1350**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-sip	OS-CIS-IOS-40416/250
Denial of Service	25-March-16	7.8	The Smart Install client implementation in Cisco IOS 12.2, 15.0, and 15.2	http://tools.cisco.com/security/center/co	OS-CIS-IOS-40416/251

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			and IOS XE 3.2 through 3.7 allows remote attackers to cause a denial of service (device reload) via crafted image list parameters in a Smart Install packet, aka Bug ID CSCuv45410. **Reference:CVE -2016-1349**	ntent/CiscoSecurityAdvisory/cisco-sa-20160323-smi	
Denial of Service	25-March-16	7.8	Cisco IOS 15.0 through 15.5 and IOS XE 3.3 through 3.16 allow remote attackers to cause a denial of service (device reload) via a crafted DHCPv6 Relay message, aka Bug ID CSCus55821. **Reference:CVE -2016-1348**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-dhcpv6	OS-CIS-IOS-40416/252
Denial of Service	25-March-16	7.1	The IKEv2 implementation in Cisco IOS 15.0 through 15.6 and IOS XE 3.3 through 3.17 allows remote attackers to cause a denial of service (device reload) via fragmented packets, aka Bug ID CSCux38417. **Reference:CVE -2016-1344**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-ios-ikev2	OS-CIS-IOS-40416/253
IOS;Nx-os *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.* *NX-OS is a network operating system for the Nexus-series Ethernet switches and MDS-series Fibre Channel storage area network switches made by Cisco System.*					
Denial of Service	25March-16	7.8	The Locator/ID Separation Protocol (LISP) implementation in Cisco IOS 15.1 and 15.2 and NX-OS 4.1 through 6.2 allows remote attackers to cause	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	OS-CIS-IOS;N-40416/254

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			a denial of service (device reload) via a crafted header in a packet, aka Bug ID CSCuu64279. **Reference:CVE -2016-1351**	20160323-lisp	
Web Security Appliance *Cisco Web Security Appliance provides exceptional web security and control for organizations of all sizes – integrated into one appliance.*					
Denial of Service	03-March-16	5	The HTTPS Proxy feature in Cisco AsyncOS before 8.5.3-051 and 9.x before 9.0.0-485 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (service outage) by leveraging certain intranet connectivity and sending a malformed HTTPS request, aka Bug ID CSCuu24840. **Reference:CVE -2016-1288**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-wsa	OS-CIS-WEB S-40416/255
Debian					
Debian Linux *Debian is an operating system and a distribution of Free Software.*					
Gain Privileges	13-March-16	7.2	pt_chown in the glibc package before 2.19-18+deb8u4 on Debian jessie lacks a namespace check associated with file-descriptor passing, which allows local users to capture keystrokes and spoof data, and possibly gain privileges, via pts read and write operations, related to debian/sysdeps/linux.mk. NOTE: this is not	http://anonscm.debian.org/cgit/pkg-glibc/glibc.git/commit/?h=jessie&id=11475c083282c1582c4dd72eecfcb2b7d308c958	OS-DEB-DEBIA-40416/256

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			considered a vulnerability in the upstream GNU C Library because the upstream documentation has a clear security recommendation against the --enable-pt_chown option. **Reference:CVE -2016-2856**		
Google					
Android *Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices .*					
Gain Information	12-March-16	4.3	The getDeviceIdForPhone function in internal/telephony/PhoneSubInfoController.java in Telephony in Android 5.x before 5.1.1 LMY49H and 6.x before 2016-03-01 does not check for the READ_PHONE_STATE permission, which allows attackers to obtain sensitive information via a crafted application, aka internal bug 25778215. **Reference:CVE -2016-0831**	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/257
Gain Information	12-March-16	5	The Widevine Trusted Application in Android 6.0.1 before 2016-03-01 allows attackers to obtain sensitive TrustZone secure-storage information by leveraging kernel access, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/258

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			20860039. **Reference:CVE -2016-0825**		
Gain Privileges	12-March-16	9.3	libcameraservice in mediaserver in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49H, and 6.x before 2016-03-01 does not require use of the ICameraService::dump method for a camera service dump, which allows attackers to gain privileges via a crafted application that directly dumps, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26265403. **Reference:CVE -2016-0826**	https://android.googlesource.com/platform/frameworks/av/+/c9ab2b0bb05a7e19fb057e79b36e232809d70122	OS-GOO-ANDRO-40416/259
Gain Privileges	12-March-16	7.6	The MediaTek connectivity kernel driver in Android 6.0.1 before 2016-03-01 allows attackers to gain privileges via a crafted application that leverages conn_launcher access, aka internal bug 25873324. **Reference:CVE -2016-0822**	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/260
Gain Privileges	12-March-16	9.3	The MediaTek Wi-Fi kernel driver in Android 6.0.1 before 2016-03-01 allows attackers to gain privileges via a crafted application, aka internal bug 26267358. **Reference:CVE -2016-0820**	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/261

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Gain Privileges	12-March-16	9.3	The Qualcomm performance component in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49H, and 6.x before 2016-03-01 allows attackers to gain privileges via a crafted application, aka internal bug 25364034. **Reference:CVE -2016-0819**	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/262
Bypass	12-March-16	6.6	Setup Wizard in Android 5.1.x before LMY49H and 6.x before 2016-03-01 allows physically proximate attackers to bypass the Factory Reset Protection protection mechanism and delete data via unspecified vectors, aka internal bug 25955042. **Reference:CVE -2016-0832**	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/263
Bypass;Gain Information	12-March-16	5	The BnGraphicBufferProducer::onTransact function in libs/gui/IGraphicBufferConsumer.cpp in mediaserver in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49H, and 6.x before 2016-03-01 does not initialize a certain output data structure, which allows attackers to obtain sensitive information, and consequently bypass an unspecified protection mechanism, by triggering a QUEUE_BUFFER action, as demonstrated by	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/264

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			obtaining Signature or SignatureOrSystem access, aka internal bug 26338109. **Reference:CVE -2016-0829**		
Bypass;Gain Information	12-March-16	5	The BnGraphicBufferConsumer::onTransact function in libs/gui/IGraphicBufferConsumer.cpp in mediaserver in Android 5.x before 5.1.1 LMY49H and 6.x before 2016-03-01 does not initialize a certain slot variable, which allows attackers to obtain sensitive information, and consequently bypass an unspecified protection mechanism, by triggering an ATTACH_BUFFER action, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 26338113. **Reference:CVE -2016-0828**	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/265
Bypass;Gain Information	12-March-16	5	libmpeg2 in libstagefright in Android 6.x before 2016-03-01 allows attackers to obtain sensitive information, and consequently bypass an unspecified protection mechanism, via crafted Bitstream data, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 25765591.	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/266

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference:CVE -2016-0824		
Denial of Service;Execute Code;Memory Corruption	12-March-16	10	The MPEG4Source::fragmentedRead function in MPEG4Extractor.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49H, and 6.x before 2016-03-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 26365349. **Reference:CVE -2016-0815**	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/267
Denial of Service;Execute Code;Overflow;Memory Corruption	12-March-16	10	libvpx in mediaserver in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49H, and 6.0 before 2016-03-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, related to libwebm/mkvparser.cpp and other files, aka internal bug 23452792. **Reference:CVE -2016-1621**	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/268
Denial of Service;Execute Code;Overflow;Memory Corruption	12-March-16	10	mediaserver in Android 6.x before 2016-03-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, related to	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/269

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			decoder/ih264d_parse_islice.c and decoder/ih264d_parse_pslice.c, aka internal bug 25928803. **Reference:CVE -2016-0816**		
Denial of Service; Overflow; Memory Corruption	12-March-16	3.3	btif_config.c in Bluetooth in Android 6.x before 2016-03-01 allows remote attackers to cause a denial of service (memory corruption and persistent daemon crash) by triggering a large number of configuration entries, and consequently exceeding the maximum size of a configuration file, aka internal bug 26071376. **Reference:CVE -2016-0830**	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/270
Overflow; Gain Privileges	12-March-16	9.3	Multiple integer overflows in libeffects in mediaserver in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49H, and 6.x before 2016-03-01 allow attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, related to EffectBundle.cpp and EffectReverb.cpp, aka internal bug 26347509. **Reference:CVE -2016-0827**	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/271
Not Avialable	12-March-16	4.3	The caching functionality in the TrustManagerImpl	https://android.googlesour	OS-GOO-ANDRO-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			class in TrustManagerImpl.java in Conscrypt in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49H, and 6.x before 2016-03-01 mishandles the distinction between an intermediate CA and a trusted root CA, which allows man-in-the-middle attackers to spoof servers by leveraging access to an intermediate CA to issue a certificate, aka internal bug 26232830. **Reference:CVE -2016-0818**	ce.com/platform/external/conscrypt/+/c4ab1b959280413fb11bf4fd7f6b4c2ba38bd779	40416/272
Google;Linux					
Android/Linux Kernel *Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices. The Linux kernel is a Unix-like computer operating system kernel.*					
Gain Information	12-March-16	2.1	The pagemap_open function in fs/proc/task_mmu.c in the Linux kernel before 3.19.3, as used in Android 6.0.1 before 2016-03-01, allows local users to obtain sensitive physical-address information by reading a pagemap file, aka Android internal bug 25739721. **Reference:CVE -2016-0823**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=ab676b7d6fbf4b294bf198fb27ade5b0e865c7ce	OS-GOO-ANDRO-40416/273
Bypass	12-March-16	5	The LIST_POISON feature in include/linux/poison.h in the Linux kernel before 4.3, as used in Android 6.0.1 before 2016-03-01,	http://source.android.com/security/bulletin/2016-03-01.html	OS-GOO-ANDRO-40416/274

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			does not properly consider the relationship to the mmap_min_addr value, which makes it easier for attackers to bypass a poison-pointer protection mechanism by triggering the use of an uninitialized list entry, aka Android internal bug 26186802, a different vulnerability than CVE-2015-3636. **Reference:CVE -2016-0821**		
HP					
Futuresmart Firmware *HP FutureSmart firmware is a unique and powerful operating system that enables your HP LaserJet enterprise devices to be more useful and productive, today and well into the future.*					
Gain Information	04-March-16	5	HP LaserJet printers and MFPs and OfficeJet Enterprise printers with firmware before 3.7.01 allow remote attackers to obtain sensitive information via unspecified vectors. **Reference:CVE -2016-2244**	https://h20565.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c05030353	OS-HP-FUTUR-40416/275
Microsoft					
Windows 10 *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems, each of which cater to a certain sector of the computing industry. Active Windows families include Windows NT, Windows Embedded and Windows Phone; these may encompass subfamilies, e.g. Windows Embedded Compact (Windows CE) or Windows Server.*					
Execute Code	09-March-16	9.3	The PDF library in Microsoft Windows 10	http://technet.microsoft.c	OS-MIC-WINDO-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Gold and 1511 allows remote attackers to execute arbitrary code via a crafted PDF document, aka "Windows Remote Code Execution Vulnerability." **Reference:CVE -2016-0118**	om/en-us/security/bulletin/ms16-028	40416/276
Windows 10;Windows 7;Windows 8.1;Windows Rt 8.1;Windows Server 2008;Windows Server 2012 *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems, each of which cater to a certain sector of the computing industry. Active Windows families include Windows NT, Windows Embedded and Windows Phone; these may encompass subfamilies, e.g. Windows Embedded Compact (Windows CE) or Windows Server.*					
Execute Code	09-March-16	9.3	Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow remote attackers to execute arbitrary code via crafted media content, aka "Windows Media Parsing Remote Code Execution Vulnerability." **Reference:CVE -2016-0101**	http://technet.microsoft.com/en-us/security/bulletin/ms16-027	OS-MIC-WINDO-40416/277
Execute Code	09-March-16	9.3	Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 allow remote attackers to execute arbitrary code via	http://technet.microsoft.com/en-us/security/bulletin/ms16-027	OS-MIC-WINDO-40416/278

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			crafted media content, aka "Windows Media Parsing Remote Code Execution Vulnerability." **Reference:CVE -2016-0098**		
Gain Privileges	09-March-16	7.2	The Secondary Logon Service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 does not properly process request handles, which allows local users to gain privileges via a crafted application, aka "Secondary Logon Elevation of Privilege Vulnerability." **Reference:CVE -2016-0099**	http://technet.microsoft.com/en-us/security/bulletin/ms16-032	OS-MIC-WINDO-40416/279
Gain Privileges	09-March-16	7.2	The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0093, CVE-2016-0094, and CVE-2016-0095.	http://technet.microsoft.com/en-us/security/bulletin/ms16-034	OS-MIC-WINDO-40416/280

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			Reference:CVE -2016-0096		
Gain Privileges	09-March-16	7.2	The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0093, CVE-2016-0094, and CVE-2016-0096. **Reference:CVE -2016-0095**	http://technet.microsoft.com/en-us/security/bulletin/ms16-034	OS-MIC-WINDO-40416/281
Gain Privileges	09-March-16	7.2	The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0093, CVE-2016-0095, and CVE-2016-0096. **Reference:CVE -2016-0094**	http://technet.microsoft.com/en-us/security/bulletin/ms16-034	OS-MIC-WINDO-40416/282
Gain Privileges	09-March-16	7.2	The kernel-mode driver in Microsoft Windows Vista SP2, Windows Server	http://technet.microsoft.com/en-	OS-MIC-WINDO-40416/283

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0094, CVE-2016-0095, and CVE-2016-0096. **Reference:CVE -2016-0093**	us/security/bulletin/ms16-034	
Denial of Service	09-March-16	7.1	The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to cause a denial of service (system hang) via a crafted OpenType font, aka "OpenType Font Parsing Vulnerability." **Reference:CVE -2016-0120**	http://technet.microsoft.com/en-us/security/bulletin/ms16-026	OS-MIC-WINDO-40416/284
Execute Code	09-March-16	9.3	The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold	http://technet.microsoft.com/en-us/security/bulletin/ms16-026	OS-MIC-WINDO-40416/285

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			and 1511 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka "OpenType Font Parsing Vulnerability." **Reference:CVE -2016-0121**		
Execute Code	09-March-16	9.3	OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka "Windows OLE Memory Remote Code Execution Vulnerability," a different vulnerability than CVE-2016-0091. **Reference:CVE -2016-0092**	http://technet.microsoft.com/en-us/security/bulletin/ms16-030	OS-MIC-WINDO-40416/286
Execute Code	09-March-16	6.8	OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka "Windows OLE Memory Remote Code Execution Vulnerability," a different vulnerability than CVE-	http://technet.microsoft.com/en-us/security/bulletin/ms16-030	OS-MIC-WINDO-40416/287

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			2016-0092. **Reference:CVE -2016-0091**		
Execute Code	09-March-16	7.2	The USB Mass Storage Class driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows physically proximate attackers to execute arbitrary code by inserting a crafted USB device, aka "USB Mass Storage Elevation of Privilege Vulnerability." **Reference:CVE -2016-0133**	http://technet.microsoft.com/en-us/security/bulletin/ms16-033	OS-MIC-WINDO-40416/288
Execute Code	09-March-16	9.3	The PDF library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted PDF document, aka "Windows Remote Code Execution Vulnerability." **Reference:CVE -2016-0117**	http://technet.microsoft.com/en-us/security/bulletin/ms16-028	OS-MIC-WINDO-40416/289
Gain Privileges	09-March-16	7.2	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 do not properly validate handles, which allows local users to gain privileges via a	http://technet.microsoft.com/en-us/security/bulletin/ms16-031	OS-MIC-WINDO-40416/290

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			crafted application, aka "Windows Elevation of Privilege Vulnerability." **Reference:CVE -2016-0087**		
Execute Code; Gain Privileges	09-March-16	7.2	Microsoft Windows Vista SP2 and Server 2008 SP2 mishandle library loading, which allows local users to gain privileges via a crafted application, aka "Library Loading Input Validation Remote Code Execution Vulnerability." **Reference:CVE -2016-0100**	http://technet.microsoft.com/en-us/security/bulletin/ms16-025	OS-MIC-WINDO-40416/291
Siemens					
Apogee Insight *Customized solution that enables you to build upon past investments, meet today's needs, and prepares you to take advantage of emerging technologies.*					
Gain Information	18-March-16	3.6	Siemens APOGEE Insight uses weak permissions for the application folder, which allows local users to obtain sensitive information or modify data via unspecified vectors. **Reference:CVE** -2016-3155	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-151221.pdf	OS-SIE-APOGE-40416/292
Operating System/Application (OS/A)					
Apple/Apple					
Apple Tv;Iphone Os/Safari *Apple TV is a digital media player and a microconsole developed and sold by Apple Inc.* *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.* *Safari is a web browser developed by Apple based on the WebKit engine.*					
Denial of Service	23-March-16	4.3	The History implementation in WebKit	https://support.apple.com/	OS-A-APP-APPLE-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			in Apple iOS before 9.3, Safari before 9.1, and tvOS before 9.2 allows remote attackers to cause a denial of service (resource consumption and application crash) via a crafted web site. **Reference:CVE -2016-1784**	HT206166	40416/293
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	9.3	WebKit in Apple iOS before 9.3, Safari before 9.1, and tvOS before 9.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference:CVE -2016-1783**	https://support.apple.com/HT206166	OS-A-APP-APPLE-40416/294
Apple Tv;Iphone Os;Mac Os X;Watchos/Safari *Apple TV is a digital media player and a microconsole developed and sold by Apple Inc. iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware. OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc. It is designed to run on Macintosh computer watchOS is the mobile operating system of the Apple Watch, developed by Apple Inc.;Safari is a web browser developed by Apple based on the WebKit engine*					
Denial of Service;Execute Code;Overflow;Memory Corruption	23-March-16	10	libxml2 in Apple iOS before 9.3, OS X before 10.11.4, Safari before 9.1, tvOS before 9.2, and watchOS before 2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document. **Reference:CVE -2016-1762**	https://support.apple.com/HT206166	OS-A-APP-APPLE-40416/295

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
Iphone Os/Safari *iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.* *Safari is a web browser developed by Apple based on the WebKit engine.*					
Bypass	23-March-16	4.3	WebKit in Apple iOS before 9.3 and Safari before 9.1 does not properly restrict redirects that specify a TCP port number, which allows remote attackers to bypass intended port restrictions via a crafted web site. **Reference:CVE -2016-1782**	https://support.apple.com/HT206171	OS-A-APP-IPHON-40416/296
Bypass;Gain Information	23-March-16	5.8	The Page Loading implementation in WebKit in Apple iOS before 9.3 and Safari before 9.1 mishandles HTTP responses with a 3xx (aka redirection) status code, which allows remote attackers to spoof the displayed URL, bypass the Same Origin Policy, and obtain sensitive cached information via a crafted web site. **Reference:CVE -2016-1786**	https://support.apple.com/HT206171	OS-A-APP-IPHON-40416/297
Bypass;Gain Information	23-March-16	4.3	The Page Loading implementation in WebKit in Apple iOS before 9.3 and Safari before 9.1 mishandles character encoding during access to cached data, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a	https://support.apple.com/HT206171	OS-A-APP-IPHON-40416/298

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			crafted web site. **Reference:CVE -2016-1785**		
Bypass;Gain Information	23-March-16	4.3	WebKit in Apple iOS before 9.3 and Safari before 9.1 allows remote attackers to bypass the Same Origin Policy and obtain physical-location data via a crafted geolocation request. **Reference:CVE -2016-1779**	https://support.apple.com/HT206171	OS-A-APP-IPHON-40416/299
Denial of Service;Execute Code;Memory Corruption	23-March-16	9.3	WebKit in Apple iOS before 9.3 and Safari before 9.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference:CVE -2016-1778**	https://support.apple.com/HT206171	OS-A-APP-IPHON-40416/300
Not Avialable	23-March-16	4.3	WebKit in Apple iOS before 9.3 and Safari before 9.1 mishandles attachment URLs, which makes it easier for remote web servers to track users via unspecified vectors. **Reference:CVE -2016-1781**	https://support.apple.com/HT205639	OS-A-APP-IPHON-40416/301
Apple/Ruby-lang					
Mac Os X/Ruby *OS X is a series of Unix-based graphical interface operating systems (OS) developed and marketed by Apple Inc. It is designed to run on Macintosh computer. A dynamic, open source programming language with a focus on simplicity and productivity.*					
Denial of Service;Execute Code	23-March-16	4.6	The Fiddle::Handle implementation in ext/fiddle/handle.c in Ruby before 2.0.0-p648,	http://bugs.debian.org/cgi-bin/bugrepor	OS-A-APP-MAC O-40416/302

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			2.1 before 2.1.8, and 2.2 before 2.2.4, as distributed in Apple OS X before 10.11.4 and other products, mishandles tainting, which allows context-dependent attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted string, related to the DL module and the libffi library. NOTE: this vulnerability exists because of a CVE-2009-5147 regression. **Reference:CVE -2015-7551**	t.cgi?bug=796344	
Fedoraproject/Fuseiso Project					
Fedora/Fuseiso *Fedora is an operating system based on the Linux kernel, developed by the community-supported Fedora Project.* *The fuseiso command line program is a simple tool that uses FUSE and helps for a regular user to mount ISO disk images.*					
Denail of Service;Execute Code;Overflow	30-March-16	5	Stack-based buffer overflow in the isofs_real_readdir function in isofs.c in FuseISO 20070708 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long pathname in an ISO file. **Reference:CVE -2015-8837**	https://bugzilla.redhat.com/show_bug.cgi?id=862211	OS-A-FED-FEDOR-40416/303
Denial of Service; Overflow	30-March-16	5	Integer overflow in the isofs_real_read_zf function in isofs.c in FuseISO 20070708 might allow	https://bugzilla.redhat.com/show_bug.cgi?	OS-A-FED-FEDOR-40416/304

[Type text]

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch(if any)	NCIIPC ID
			remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a large ZF block size in an ISO file, leading to a heap-based buffer overflow. **Reference:CVE -2015-8836**	id=861358	