National Critical Information Infrastructure Protection Centre

CVE Report

01- 15 May 2016

Vol. 3 No.8

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Application					
Accellion					
File Transfer Appliance *Use the Pegasystems File Transfer Appliance (FTA) to upload large files to Pegasystems Global Customer Support (GCS).*					
Execute Code	07-May-2016	6.5	The Accellion File Transfer Appliance (FTA) before FTA_9_12_40 allows remote authenticated users to execute arbitrary commands by leveraging the YUM_CLIENT restricted-user role. **Reference:CVE-2016-2352**	NA	A-ACC-FILE -180516/1
Execute Code; Sql Injection	07-May-2016	7.5	SQL injection vulnerability in home/seos/courier/security_key2.api on the Accellion File Transfer Appliance (FTA) before FTA_9_12_40 allows remote attackers to execute arbitrary SQL commands via the client_id parameter. **Reference:CVE-2016-2351**	NA	A-ACC-FILE -180516/2
Cross Site Scripting	07-May-2016	4.3	Multiple cross-site scripting (XSS) vulnerabilities on the Accellion File Transfer Appliance (FTA) before FTA_9_12_40 allow remote attackers to inject arbitrary web script or	NA	A-ACC-FILE -180516/3

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			HTML via unspecified input to (1) NA getimageajax.php, (2) move_partition_frame.html, or (3) wmInfo.html. **Reference:CVE-2016-2350**		
Adobe					
Acrobat Dc;Acrobat Reader Dc;Acrobat Xi;Reader Xi *Adobe Acrobat Reader DC software is the free global standard for reliably viewing, printing, and commenting on PDF documents. Adobe Acrobat DC is a trusted PDF creator. Foxit Reader is a lightweight, fast, and secure PDF Reader capable of high-volume processing. Acrobat is used to convert, edit and sign PDF files at your desk or on the go.Adobe Reader XI is software that allows you to reliably view, print and comment PDF documents.*					
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1121**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/4
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/5

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors **Reference:CVE-2016-1094**		
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1075**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/6
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/7

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1070**		
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1069**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/8
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1068**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/9

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1067**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/10
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1066**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/11
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/12

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1065**		
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1061**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/13
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/14

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1060**		
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1059**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/15
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/16

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			vectors. **Reference:CVE-2016-1058**		
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1057**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/17
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1056**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/18
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe	https://helpx.adobe.com/se	A-ADO-ACROB-180516/19

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1055**	curity/products/acrobat/apsb16-14.html	
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1054**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/20
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172,	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/21

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors **Reference:CVE-2016-1053**		
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1052**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/22
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/23

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1051**		
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1050**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/24
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/25

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			2016-1049		
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1048**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/26
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1047**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/27
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16,	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACROB-180516/28

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors.. **Reference:CVE-2016-1046**	b16-14.html	
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-1045**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/29
Acrobat;Acrobat Dc;Acrobat Reader Dc;Reader *Adobe Acrobat Reader DC software is the free global standard for reliably viewing, printing, and commenting on PDF documents. Adobe Acrobat DC is a trusted PDF creator.Foxit Reader is a lightweight, fast, and secure PDF Reader capable of high-volume processing. Acrobat is used to convert, edit and sign PDF files at your desk or on the go.*					
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16,	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACROB-180516/30

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors.. **Reference:CVE-2016-4107**	b16-14.html	
Gain Previleges	11-May-2016	7.2	Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows local users to gain privileges via a Trojan horse resource in an unspecified directory, a different vulnerability than CVE-2016-1087 and CVE-2016-1090. **Reference:CVE-2016-4106**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/31
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/32

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4105**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4104**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/33
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/34

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4103**		
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors. **Reference:CVE-2016-4102**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/35
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/36

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4101**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4100**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/37
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/38

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4099**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4098**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/39
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/40

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4097**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors **Reference:CVE-2016-4096**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/41
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/42

Product/ Vulnerability Type(s)	**Publish Date**	**CVSS**	**Vulnerability Description**	**Patch (if any)**	**NCIIPC ID**
			execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4094**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4093**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/43
Execute Code; Overflow	11-May-2016	10	Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/44

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4091. **Reference:CVE-2016-4092**		
Execute Code; Overflow	11-May-2016	10	Heap-based buffer overflow in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4092. **Reference:CVE-2016-4091**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/45
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/46

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4090**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-4089**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/47
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/48

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			(memory corruption) via unspecified vectors. **Reference:CVE-2016-4088**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors **Reference:CVE-2016-1130**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/49
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption)	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/50

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			via unspecified vectors. **Reference:CVE-2016-1129**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1128**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/51
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/52

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			vectors. **Reference:CVE-2016-1127**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1126**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/53
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/54

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Reference:CVE-2016-1125		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1124**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/55
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/56

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			2016-1123		
Execute Code	11-May-2016	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors **Reference:CVE-2016-1122**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/57
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors **Reference:CVE-2016-1120**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/58
Denial of Service; Execute Code;	11-May-2016	10	Adobe Reader and Acrobat before	https://helpx.adobe.com/se	A-ADO-ACROB-180516/59

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Overflow; Memory Corruption			11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1119**	curity/products/acrobat/apsb16-14.html	
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1118**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/60
Bypass	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and	https://helpx.adobe.com/security/product	A-ADO-ACROB-180516/61

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors. **Reference:CVE-2016-1117**	s/acrobat/apsb16-14.html	
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1116**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/62
Gain Information	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/63

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to obtain sensitive information via unspecified vectors. **Reference:CVE-2016-1112**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1095**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/64
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/65

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1093**		
Gain Information	11-May-2016	5	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to obtain sensitive information from process memory via unspecified vectors, a different vulnerability than CVE-2016-1079. **Reference:CVE-2016-1092**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/66
Gain Privileges	11-May-2016	7.2	Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/67

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Windows and OS X allows local users to gain privileges via a Trojan horse resource in an unspecified directory, a different vulnerability than CVE-2016-1087 and CVE-2016-4106. **Reference:CVE-2016-1090**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors **Reference:CVE-2016-1088**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/68
Gain Privileges	11-May-2016	7.2	Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/69

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			15.016.20039 on Windows and OS X allows local users to gain privileges via a Trojan horse resource in an unspecified directory, a different vulnerability than CVE-2016-1090 and CVE-2016-4106. **Reference:CVE-2016-1087**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1086**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/70
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/71

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1085**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors **Reference:CVE-2016-1084**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/72
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/73

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1083**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1082**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/74
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/75

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors **Reference:CVE-2016-1081**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors., **Reference:CVE-2016-1080**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/76
Gain Information	11-May-2016	5	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/77

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			obtain sensitive information from process memory via unspecified vectors, a different vulnerability than CVE-2016-1092. **Reference:CVE-2016-1079**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors **Reference:CVE-2016-1078**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/78
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/79

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1077**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1076**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/80
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/81

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1074**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors **Reference:CVE-2016-1073**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/82
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/83

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			(memory corruption) via unspecified vectors. **Reference:CVE-2016-1072**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1071**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/84
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption)	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/85

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			via unspecified vectors. **Reference:CVE-2016-1064**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1063**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/86
Bypass	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors **Reference:CVE-**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/87

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			2016-1062		
Bypass	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1062, and CVE-2016-1117.	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/88
			Reference:CVE-2016-1044		
Execute Code; Overflow	11-May-2016	10	Integer overflow in Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allows attackers to execute arbitrary	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/89

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			code via unspecified vectors. **Reference:CVE-2016-1043**		
Bypass	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1044, CVE-2016-1062, and CVE-2016-1117. **Reference:CVE-2016-1042**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/90
Bypass	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/91

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1042, CVE-2016-1044, CVE-2016-1062, and CVE-2016-1117. **Reference:CVE-2016-1041**		
Bypass	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1039, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, CVE-2016-1062, and CVE-2016-1117. **Reference:CVE-2016-1040**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/92

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Bypass	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2016-1038, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, CVE-2016-1062, and CVE-2016-1117. **Reference:CVE-2016-1039**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/93
Bypass	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/94

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			vectors, a different vulnerability than CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, CVE-2016-1062, and CVE-2016-1117. **Reference:CVE-2016-1038**		
Denial of Service; Execute Code; Overflow; Memory Corruption	11-May-2016	10	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference:CVE-2016-1037**	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-180516/95
Coldfusion *ColdFusion is a commercial rapid web application development platform created by JJ Allaire in 1995.*					
NA	10-May-2016	5.8	Adobe ColdFusion 10 before Update 19, 11 before Update 8, and 2016 before Update 1 mishandles wildcards in name fields of X.509 certificates, which might allow	https://helpx.adobe.com/security/products/coldfusion/apsb16-16.html	A-ADO-COLDF-180516/96

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			man-in-the-middle attackers to spoof servers via a crafted certificate. **Reference:CVE-2016-1115**		
Execute Code	10-May-2016	7.5	Adobe ColdFusion 10 before Update 19, 11 before Update 8, and 2016 before Update 1 allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library. **Reference:CVE-2016-1114**	https://helpx.adobe.com/security/products/coldfusion/apsb16-16.html	A-ADO-COLDF-180516/97
Cross Site Scripting	10-May-2016	4.3	Cross-site scripting (XSS) vulnerability in Adobe ColdFusion 10 before Update 19, 11 before Update 8, and 2016 before Update 1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference:CVE-2016-1113**	https://helpx.adobe.com/security/products/coldfusion/apsb16-16.html	A-ADO-COLDF-180516/98
Flash Player *Cross-platform plugin plays animations, videos and sound files in .SWF format.*					
Execute Code	10-May-2016	10	Adobe Flash Player 21.0.0.226 and earlier allows remote attackers to execute arbitrary code via unspecified vectors,	https://helpx.adobe.com/security/products/flash-player/apsa16-02.html	A-ADO-FLASH-180516/99

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			as exploited in the wild in May 2016. **Reference:CVE-2016-4117**		
Adobe;Microsoft					
Flash Player/Edge;Internet Explorer *Cross-platform plugin plays animations, videos and sound files in .SWF format. Internet Explorer is the world's most popular Web browser.EDGE (also known as Enhanced GPRS or EGPRS) is a data system used on top of GSM networks.*					
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-4116**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/100
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-4115**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/101

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-4114**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/102
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-4113**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/103
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge,	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/104

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-4112**		
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-4111**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/105
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-4110**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/106
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe	http://technet.microsoft.co	A-ADO-FLASH-180516/107

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-4109**	m/en-us/security/bulletin/ms16-064	
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-4108**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/108
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/109

Product/ Vulnerability Type(s)	**Publish Date**	**CVSS**	**Vulnerability Description**	**Patch (if any)**	**NCIIPC ID**
			different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1110**		
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1109**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/110
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1108**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/111
NA	11-May-2016	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and	http://technet.microsoft.com/en-us/security/bu	A-ADO-FLASH-180516/112

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1107**	lletin/ms16-064	
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1106**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/113
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/114

Product/ Vulnerability Type(s)	**Publish Date**	**CVSS**	**Vulnerability Description**	**Patch (if any)**	**NCIIPC ID**
			in MS16-064. **Reference:CVE-2016-1105**		
NA	11-May-2016	9.3	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1104**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/115
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1103**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/116
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/117

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1102**		
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1101**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/118
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/119

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			2016-1100		
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1099**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/120
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1098**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/121
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/122

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1097**		
NA	11-May-2016	7.6	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064. **Reference:CVE-2016-1096**	http://technet.microsoft.com/en-us/security/bulletin/ms16-064	A-ADO-FLASH-180516/123
Apache					
Cordova *Apache Cordova (formerly PhoneGap) is a popular mobile application development framework originally created by Nitobi.*					
Bypass	09-May-2016	7.5	Apache Cordova iOS before 4.0.0 might allow attackers to bypass a URL whitelist protection mechanism in an app and load arbitrary resources by leveraging unspecified methods. **Reference:CVE-2015-5207**	https://cordova.apache.org/announcements/2016/04/27/security.html	A-APA-CORDO-180516/124
Subversion *Apache Subversion is a software versioning and revision control system distributed as free software*					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
under the Apache License.					
Denial of Service	05-May-2016	4	The req_check_access function in the mod_authz_svn module in the httpd server in Apache Subversion before 1.8.16 and 1.9.x before 1.9.4 allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) via a crafted header in a (1) MOVE or (2) COPY request, involving an authorization check. **Reference:CVE-2016-2168**	http://subversion.apache.org/security/CVE-2016-2168-advisory.txt	A-APA-SUBVE-180516/125
Bypass	05-May-2016	4.9	The canonicalize_username function in svnserve/cyrus_auth.c in Apache Subversion before 1.8.16 and 1.9.x before 1.9.4, when Cyrus SASL authentication is used, allows remote attackers to authenticate and bypass intended access restrictions via a realm string that is a prefix of an expected repository realm string. **Reference:CVE-2016-2167**	http://subversion.apache.org/security/CVE-2016-2167-advisory.txt	A-APA-SUBVE-180516/126

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Cloud Network Automation Provisioner					
Execute Code; Sql Injection	11-May-2016	6.5	SQL injection vulnerability in Cisco Cloud Network Automation Provisioner (CNAP) 1.0 and 1.1 allows remote authenticated users to execute arbitrary SQL commands via a crafted URL, aka Bug ID CSCuy72175. **Reference:CVE-2016-1393**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160510-cnap	A-CIS-CLOUD-180516/127
Finesse *Cisco Finesse is a next-generation agent and supervisor desktop designed to provide a collaborative experience for the various communities that interact with your customer service organization. It helps improve the customer experience while offering a user-centric design to enhance customer care representative satisfaction as well.*					
NA	05-May-2016	5	The gadgets-integration API in Cisco Finesse 8.5(1) through 8.5(5), 8.6(1), 9.0(1), 9.0(2), 9.1(1), 9.1(1)SU1, 9.1(1)SU1.1, 9.1(1)ES1 through 9.1(1)ES5, 10.0(1), 10.0(1)SU1, 10.0(1)SU1.1, 10.5(1), 10.5(1)ES1 through 10.5(1)ES4, 10.5(1)SU1, 10.5(1)SU1.1, 10.5(1)SU1.7, 10.6(1), 10.6(1)SU1, 10.6(1)SU2, and 11.0(1) allows remote attackers to conduct server-side request forgery (SSRF) attacks	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-finesse	A-CIS-FINES-180516/128

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			via a crafted request, aka Bug ID CSCuw86623. **Reference:CVE-2016-1373**		
Firesight System Software *Cisco FireSIGHT System Software 5.4.0 through 6.0.1 and ASA with FirePOWER Services 5.4.0 through 6.0.0.1 allow remote attackers to bypass malware protection via crafted fields in HTTP headers, aka Bug ID CSCux22726.*					
Denial of Service	05-May-2016	7.8	Cisco FirePOWER System Software 5.3.x through 5.3.0.6 and 5.4.x through 5.4.0.3 on FirePOWER 7000 and 8000 appliances, and on the Advanced Malware Protection (AMP) for Networks component on these appliances, allows remote attackers to cause a denial of service (packet-processing outage) via crafted packets, aka Bug ID CSCuu86214. **Reference:CVE-2016-1368**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-firepower	A-CIS-FIRES-180516/129
Prime Collaboration Assurance *Cisco Prime Collaboration provides automated and accelerated provisioning, real-time monitoring, proactive troubleshooting, and long-term trending and analytics in one integrated product.*					
NA	05-May-2016	5.8	Open redirect vulnerability in Cisco Prime Collaboration Assurance Software 10.5 through 11.0 allows remote attackers to redirect users to arbitrary web sites and conduct	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160503-pca	A-CIS-PRIME-180516/130

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			phishing attacks via unspecified vectors, aka Bug ID CSCuu34121. **Reference:CVE-2016-1392**		
Telepresence Tc Software *Cisco TelePresence TC software-based endpoints provide two options natively for creating a system backup. The first option involves amassing the output data of the configuration settings through the CLI. The second method is a new feature that enables an administrator to perform a backup using the web interface.*					
Execute Code	05-May-2016	9	The XML API in TelePresence Codec (TC) 7.2.0, 7.2.1, 7.3.0, 7.3.1, 7.3.2, 7.3.3, 7.3.4, and 7.3.5 and Collaboration Endpoint (CE) 8.0.0, 8.0.1, and 8.1.0 in Cisco TelePresence Software mishandles authentication, which allows remote attackers to execute control commands or make configuration changes via an API request, aka Bug ID CSCuz26935. **Reference:CVE-2016-1387**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-tpxml	A-CIS-TELEP-180516/131
EMC					
Rsa Authentication Manager *Authentication Manager enables RSA SecurID administrators to centrally manage user profiles and authentication methods as well as applications and agents across multiple physical sites.*					
Http R.Spl.	07-May-2016	5	CRLF injection vulnerability in EMC RSA Authentication Manager before 8.1 SP1 P14 allows remote attackers to	http://seclists.org/bugtraq/2016/May/23	A-EMC-RSA A-180516/132

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors. **Reference:CVE-2016-0902**		
Cross Site Scripting	07-May-2016	4.3	Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Manager before 8.1 SP1 P14 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-0900. **Reference:CVE-2016-0901**	http://seclists.org/bugtraq/2016/May/23	A-EMC-RSA A-180516/133
Cross Site Scripting	07-May-2016	4.3	Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Manager before 8.1 SP1 P14 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-0901. **Reference:CVE-2016-0900**	http://seclists.org/bugtraq/2016/May/23	A-EMC-RSA A-180516/134
NA	03-May-2016	4.3	EMC RSA Data Loss Prevention 9.6 before SP2 P5 allows remote attackers to conduct clickjacking attacks via web-site elements	http://seclists.org/bugtraq/2016/May/9	A-EMC-RSA D-180516/135

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			with crafted transparency or opacity. **Reference:CVE-2016-0895**		
Bypass	03-May-2016	6.5	EMC RSA Data Loss Prevention 9.6 before SP2 P5 allows remote authenticated users to bypass intended object access restrictions via a modified parameter. **Reference:CVE-2016-0894**	http://seclists.org/bugtraq/2016/May/9	A-EMC-RSA D-180516/136
Gain Information	03-May-2016	4	EMC RSA Data Loss Prevention 9.6 before SP2 P5 allows remote authenticated users to obtain sensitive information by reading error messages. **Reference:CVE-2016-0893**	http://seclists.org/bugtraq/2016/May/9	A-EMC-RSA D-180516/137
Cross Site Scripting	03-May-2016	4.3	Cross-site scripting (XSS) vulnerability in EMC RSA Data Loss Prevention 9.6 before SP2 P5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference:CVE-2016-0892**	http://seclists.org/bugtraq/2016/May/9	A-EMC-RSA D-180516/138
HP					
Network Node Manager I *HPE Network Node Manager i (NNMi) software provides powerful out-of- the-box capabilities that enable your network operations team to efficiently.*					
Gain Information	07-May-	4	HPE Network Node	https://h2056	A-HP-NETWO-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
	2016		Manager i (NNMi) 9.20, 9.23, 9.24, 9.25, 10.00, and 10.01 allows remote authenticated users to obtain sensitive information via unspecified vectors. **Reference:CVE-2016-2013**	4.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05103564	180516/139
Bypass	07-May-2016	7.5	HPE Network Node Manager i (NNMi) 9.20, 9.23, 9.24, 9.25, 10.00, and 10.01 allows remote attackers to bypass authentication via unspecified vectors. **Reference:CVE-2016-2012**	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05103564	A-HP-NETWO-180516/140
Cross Site Scripting	07-May-2016	3.5	Cross-site scripting (XSS) vulnerability in HPE Network Node Manager i (NNMi) 9.20, 9.23, 9.24, 9.25, 10.00, and 10.01 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-2010. **Reference:CVE-2016-2011**	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05103564	A-HP-NETWO-180516/141
Cross Site Scripting	07-May-2016	3.5	Cross-site scripting (XSS) vulnerability in HPE Network Node Manager i (NNMi) 9.20, 9.23, 9.24, 9.25, 10.00, and 10.01	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_n	A-HP-NETWO-180516/142

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-2011. **Reference:CVE-2016-2010**	a-c05103564	
Execute Code	07-May-2016	6.5	HPE Network Node Manager i (NNMi) 9.20, 9.23, 9.24, 9.25, 10.00, and 10.01 allows remote authenticated users to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library. **Reference:CVE-2016-2009**	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05103564	A-HP-NETWO-180516/143
Imagemagick					
Imagemagick *ImageMagick is a software suite to create, edit, compose, or convert bitmap images.*					
Gain Information	05-May-2016	7.1	The LABEL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to read arbitrary files via a crafted image. **Reference:CVE-2016-3717**	http://git.imagemagick.org/repos/ImageMagick/blob/a01518e08c840577cabd7d3ff291a9ba735f7276/ChangeLog	A-IMA-IMAGE-180516/144
NA	05-May-2016	4.3	The MSL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to	https://www.imagemagick.org/discourse-server/viewtopic.php?	A-IMA-IMAGE-180516/145

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			move arbitrary files via a crafted image. **Reference:CVE-2016-3716**	f=4&t=29588	
NA	05-May-2016	5.8	The EPHEMERAL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to delete arbitrary files via a crafted image. **Reference:CVE-2016-3715**	http://git.imagemagick.org/repos/ImageMagick/blob/a01518e08c840577cabd7d3ff291a9ba735f7276/ChangeLog	A-IMA-IMAGE-180516/146
Execute Code	05-May-2016	10	The (1) EPHEMERAL, (2) HTTPS, (3) MVG, (4) MSL, (5) TEXT, (6) SHOW, (7) WIN, and (8) PLT coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to execute arbitrary code via shell metacharacters in a crafted image, aka "ImageTragick." **Reference:CVE-2016-3714**	https://access.redhat.com/security/vulnerabilities/2296071	A-IMA-IMAGE-180516/147
Jboss					
Enterprise Application Platform *The JBoss Enterprise Application Platform (or JBoss EAP) is a subscription-based/open-source Java EE-based application server runtime platform used for building, deploying, and hosting highly-transactional Java applications and services.*					
Denial of Service	06-May-2016	5	The HTTPS NIO Connector allows remote attackers to cause a denial of service (thread consumption) by	https://bugzilla.redhat.com/show_bug.cgi?id=1308465	A-JBO-ENTER-180516/148

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			opening a socket and not sending an SSL handshake, aka a read-timeout vulnerability. **Reference:CVE-2016-2094**		
Jq Project					
JQ *jq is like sed for JSON data - you can use it to slice and filter and map and transform structured data*					
Denial of Service; Overflow	06-May-2016	7.8	The jv_dump_term function in jq 1.5 allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted JSON file. **Reference:CVE-2016-4074**		A-JQ -JQ-180516/149
Libarchive					
Libarchive *Libarchive is a programming library that can create and read several different streaming archive formats, including most popular tar variants, several cpio formats, and both BSD and GNU ar variants.*					
Execute Code; Overflow	07-May-2016	6.8	Heap-based buffer overflow in the zip_read_mac_metadata function in archive_read_support_format_zip.c in libarchive before 3.2.0 allows remote attackers to execute arbitrary code via crafted entry-size values in a ZIP archive. **Reference:CVE-2016-1541**	https://github.com/libarchive/libarchive/commit/d0331e8e5b05b475f20b1f3101fe1ad772d7e7e7	A-LIB-LIBAR-180516/150
Littlecms					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Little Cms Color Engine *Little CMS or LCMS is an open source color management system, released as a software library for use in other programs which will allow the use of International Color Consortium profiles. It is licensed under the terms of theMIT License.*					
Execute Code	07-May-2016	10	Double free vulnerability in the DefaultICCintents function in cmscnvrt.c in liblcms2 in Little CMS 2.x before 2.6 allows remote attackers to execute arbitrary code via a malformed ICC profile that triggers an error in the default intent handler. **Reference:CVE-2013-7455**	https://github.com/mm2/Little-CMS/commit/fefaaa43c382eee632ea3ad0cfa915335140e1db	A-LIT-LITTL-180516/151
Mcafee					
Livesafe *McAfee LiveSafe service provides trusted protection so you can shop, surf and keep all your devices secure online with the convenience of a single subscription*					
Denial of Service; Memory Corruption	05-May-2016	7.8	Integer signedness error in the AV engine before DAT 8145, as used in McAfee LiveSafe 14.0, allows remote attackers to cause a denial of service (memory corruption and crash) via a crafted packed executable. **Reference:CVE-2016-4535**		A-MCA-LIVES-180516/152
Microsoft					
.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 .NET and Visual Studio. Download .NET Framework4.6.1Other versions.*					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Gain Information	10-May-2016	4.3	Microsoft .NET Framework 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, and 4.6.1 allows man-in-the-middle attackers to obtain sensitive cleartext information via vectors involving injection of cleartext data into the client-server data stream, aka "TLS/SSL Information Disclosure Vulnerability." **Reference:CVE-2016-0149**	http://technet.microsoft.com/en-us/security/bulletin/ms16-065	A-MIC-.NET-180516/153
Edge *EDGE (also known as Enhanced GPRS or EGPRS) is a data system used on top of GSM networks.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	10-May-2016	7.6	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0186 and CVE-2016-0191. **Reference:CVE-2016-0193**	http://technet.microsoft.com/en-us/security/bulletin/ms16-052	A-MIC-EDGE-180516/154
Denial of Service; Execute Code; Overflow; Memory Corruption	10-May-2016	7.6	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or	http://technet.microsoft.com/en-us/security/bulletin/ms16-	A-MIC-EDGE-180516/155

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0186 and CVE-2016-0193. **Reference:CVE-2016-0191**	052	
Denial of Service; Execute Code; Overflow; Memory Corruption	10-May-2016	7.6	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0191 and CVE-2016-0193. **Reference:CVE-2016-0186**	http://technet.microsoft.com/en-us/security/bulletin/ms16-052	A-MIC-EDGE-180516/156
Edge;Internet Explorer *Internet Explorer is the world's most popular Web browser.EDGE (also known as Enhanced GPRS or EGPRS) is a data system used on top of GSM networks.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	10-May-2016	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		A-MIC-EDGE;-180516/157

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." **Reference:CVE-2016-0192**		
Internet Explorer *Internet Explorer is the world's most popular Web browser.*					
Bypass; Gain Information	10-May-2016	2.6	Microsoft Internet Explorer 10 and 11 allows remote attackers to bypass file permissions and obtain sensitive information via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability." **Reference:CVE-2016-0194**	http://technet.microsoft.com/en-us/security/bulletin/ms16-051	A-MIC-INTER-180516/158
Bypass	10-May-2016	9.3	The User Mode Code Integrity (UMCI) implementation in Device Guard in Microsoft Internet Explorer 11 allows remote attackers to bypass a code-signing protection mechanism via unspecified vectors, aka "Internet Explorer Security Feature Bypass." **Reference:CVE-2016-0188**	http://technet.microsoft.com/en-us/security/bulletin/ms16-051	A-MIC-INTER-180516/159
Jscript;Vbscript *JScript is Microsoft's dialect of the ECMAScript standard that is used in Microsoft's Internet Explorer. JScript is implemented as an Active Scripting engine.VBScript ("Visual Basic Scripting Edition") is an Active Scripting language developed by Microsoft that is modeled on Visual Basic. It is designed as a "lightweight" language with a fast interpreter for use in a wide variety of Microsoft environments.*					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Denial of Service; Execute Code; Overflow; Memory Corruption	10-May-2016	7.6	The Microsoft (1) JScript 5.8 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0187. **Reference:CVE-2016-0189**		A-MIC-JSCRI-180516/160
Denial of Service; Execute Code; Overflow; Memory Corruption	10-May-2016	7.6	The Microsoft (1) JScript 5.8 and (2) VBScript 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0189. **Reference:CVE-2016-0187**		A-MIC-JSCRI-180516/161
Office					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Microsoft Office is an office suite of applications, servers, and services developed by Microsoft					
Execute Code; Overflow; Memory Corruption	10-May-2016	9.3	Microsoft Office 2013 SP1, 2013 RT SP1, and 2016 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference:CVE-2016-0126**	http://technet.microsoft.com/en-us/security/bulletin/ms16-054	A-MIC-OFFIC-180516/162
Office;Office Compatibility Pack;Word;Word For Mac;Word Viewer *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft. Microsoft Office Compatibility Pack is an add-on for Microsoft Office 2000, Office XP and Office 2003. Microsoft Word is a word processor developed by Microsoft. It was first released on October 25, 1983 under the name Multi-Tool Word for Xenix systems.Microsoft Office for Mac gives you new versions of Word, Excel, PowerPoint, Outlook, and OneNote that are thoughtfully designed for Mac.Microsoft Word Viewer is a freeware program for Microsoft Windows that can display and print Microsoft Word documents.*					
Execute Code; Overflow; Memory Corruption	10-May-2016	9.3	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference:CVE-2016-0198**	http://technet.microsoft.com/en-us/security/bulletin/ms16-054	A-MIC-OFFIC-180516/163

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Office;Office Web Apps;Sharepoint Server *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft*					
Execute Code; Overflow; Memory Corruption	10-May-2016	9.3	Microsoft Office 2007 SP3, Office 2010 SP2, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference:CVE-2016-0140**	http://technet.microsoft.com/en-us/security/bulletin/ms16-054	A-MIC-OFFIC-180516/164
Office;Office Web Apps;Sharepoint Server;Word *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft. Office Online (previously Office Web Apps) is an online office suite offered by Microsoft, which allows users to create and edit files using lightweight, web browser-based versions of Microsoft Office applications: Word, Excel, PowerPoint and OneNote. SharePoint is a web application platform in the Microsoft Office server suite. Microsoft Word is a word processor developed by Microsoft.*					
Execute Code	10-May-2016	9.3	The Windows font library in Microsoft Office 2010 SP2, Word 2010 SP2, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Microsoft Office Graphics RCE Vulnerability." **Reference:CVE-**	http://technet.microsoft.com/en-us/security/bulletin/ms16-054	A-MIC-OFFIC-180516/165

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			2016-0183		
Openssl					
Openssl *In computer networking, 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. It has found wide use in internet web servers, serving a majority of all web sites.*					
Denial of Service; Overflow; Gain Information	04-May-2016	6.4	The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data. **Reference:CVE-2016-2176**	https://www.openssl.org/news/secadv/20160503.txt	A-OPE-OPENS-180516/166
Denial of Service	04-May-2016	7.8	The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding. **Reference:CVE-2016-2109**	https://www.openssl.org/news/secadv/20160503.txt	A-OPE-OPENS-180516/167

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Denial of Service; Execute Code; Overflow; Memory Corruption	04-May-2016	10	The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue. **Reference:CVE-2016-2108**	https://git.openssl.org/?p=openssl.git;a=commit;h=3661bb4e7934668bd99ca777ea8b30eedfafa871	A-OPE-OPENS-180516/168
Gain Information	04-May-2016	2.6	The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session, NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169. **Reference:CVE-2016-2107**	https://www.openssl.org/news/secadv/20160503.txt	A-OPE-OPENS-180516/169
Denial of Service; Overflow; Memory Corruption	04-May-2016	5	Integer overflow in the EVP_EncryptUpdate	https://www.openssl.org/news/secadv/20	A-OPE-OPENS-180516/170

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data. **Reference:CVE-2016-2106**	160503.txt	
Denial of Service; Overflow; Memory Corruption	04-May-2016	5	Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data. **Reference:CVE-2016-2105**	https://www.openssl.org/news/secadv/20160503.txt	A-OPE-OPENS-180516/171
NA	04-May-2016	5	crypto/rsa/rsa_gen.c in OpenSSL before 0.9.6 mishandles C bitwise-shift operations that exceed the size of an expression, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by leveraging improper	https://git.openssl.org/?p=openssl.git;a=commit;h=db82b8f9bd432a59aea8e1014694e15fc457c2bb	A-OPE-OPENS-180516/172

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			RSA key generation on 64-bit HP-UX platforms. **Reference:CVE-2000-1254**		
Panasonic					
Fpwin Pro *FPWIN Pro is the universal programming software for all Panasonic PLCs.*					
Denial of Service; Overflow	11-May-2016	4.4	Heap-based buffer overflow in Panasonic FPWIN Pro 5.x through 7.x before 7.130 allows local users to cause a denial of service (application crash) via unspecified vectors. **Reference:CVE-2016-4499**		A-PAN-FPWIN-180516/173
Denial of Service	11-May-2016	6.8	Panasonic FPWIN Pro 5.x through 7.x before 7.130 accesses an uninitialized pointer, which allows local users to cause a denial of service or possibly have unspecified other impact via unknown vectors. **Reference:CVE-2016-4498**		A-PAN-FPWIN-180516/174
Denial of Service	11-May-2016	6.8	Panasonic FPWIN Pro 5.x through 7.x before 7.130 allows local users to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type		A-PAN-FPWIN-180516/175

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			confusion." **Reference:CVE-2016-4497**		
Denial of Service; Overflow	11-May-2016	4.4	Panasonic FPWIN Pro 5.x through 7.x before 7.130 allows local users to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by triggering a crafted index value, as demonstrated by an integer overflow. **Reference:CVE-2016-4496**		A-PAN-FPWIN-180516/176
Trend Micro					
Email Encryption Gateway *Symantec Gateway Email Encryption provides network-based email encryption so your emails stay secure regardless of your recipients' email infrastructure.*					
Execute Code; Sql Injection	05-May-2016	7.5	SQL injection vulnerability in the authentication functionality in Trend Micro Email Encryption Gateway (TMEEG) 5.5 before build 1107 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. **Reference:CVE-2016-4351**	https://esupport.trendmicro.com/solution/en-US/1114060.aspx	A-TRE-EMAIL-180516/177
Veritas					
Netbackup;Netbackup Appliance *Veritas NetBackup (earlier Symantec NetBackup) is an enterprise level heterogeneous backup and recovery suite. It provides cross-platform backup functionality to a large variety of Windows, UNIX and Linux operating systems.; .NetBackup Appliances give organizations an efficient turnkey solution for backup, storage, and deduplication.*					

Product/ Vulnerability Type(s)	**Publish Date**	**CVSS**	**Vulnerability Description**	**Patch (if any)**	**NCIIPC ID**
NA	07-May-2016	10	The management-services protocol implementation in Veritas NetBackup 7.x through 7.5.0.7, 7.6.0.x through 7.6.0.4, 7.6.1.x through 7.6.1.2, and 7.7.x before 7.7.2 and NetBackup Appliance through 2.5.4, 2.6.0.x through 2.6.0.4, 2.6.1.x through 2.6.1.2, and 2.7.x before 2.7.2 allows remote attackers to make arbitrary RPC calls via unspecified vectors. **Reference:CVE-2015-6552**	https://www.veritas.com/content/support/en_US/security/VTS16-001.html	A-VER-NETBA-180516/178
Gain Information	07-May-2016	4.3	Veritas NetBackup 7.x through 7.5.0.7 and 7.6.0.x through 7.6.0.4 and NetBackup Appliance through 2.5.4 and 2.6.0.x through 2.6.0.4 do not use TLS for administration-console traffic to the NBU server, which allows remote attackers to obtain sensitive information by sniffing the network for key-exchange packets. **Reference:CVE-2015-6551**	https://www.veritas.com/content/support/en_US/security/VTS16-001.html	A-VER-NETBA-180516/179
Execute Code	07-May-	10	bpcd in Veritas	https://www.v	A-VER-NETBA-

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
	2016		NetBackup 7.x through 7.5.0.7, 7.6.0.x through 7.6.0.4, 7.6.1.x through 7.6.1.2, and 7.7.x before 7.7.2 and NetBackup Appliance through 2.5.4, 2.6.0.x through 2.6.0.4, 2.6.1.x through 2.6.1.2, and 2.7.x before 2.7.2 allows remote attackers to execute arbitrary commands via crafted input. **Reference:CVE-2015-6550**	eritas.com/content/support/en_US/security/VTS16-001.html	180516/180
W1.fi					
Hostapd *Hostapd (Host access point daemon) is a user space software access point capable of turning normal network interface cards into access points and authentication servers*					
Denial of Service	09-May-2016	5	hostapd 0.6.7 through 2.5 and wpa_supplicant 0.6.7 through 2.5 do not reject \n and \r characters in passphrase parameters, which allows remote attackers to cause a denial of service (daemon outage) via a crafted WPS operation. **Reference:CVE-2016-4476**	http://www.openwall.com/lists/oss-security/2016/05/03/12	A-W1.-HOSTA-180516/181
Application/Operating System					
Botan Project/Debian					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Botan/Debian Linux					
Debian is an operating system and a distribution of Free Software.Botan is a crypto library that provides a wide variety of cryptographic algorithms, formats, and protocols.					
Denial of Service	2016-05-13	7.8	The BER decoder in Botan 1.10.x before 1.10.10 and 1.11.x before 1.11.19 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors, related to a length field. **Reference:CVE-2015-5727**	http://botan.randombit.net/security.html	A-BOT-BOTAN-180516/182
Jq Project/Novell					
JQ/Leap;Opensuse					
LEAP, the Long range Energy Alternatives Planning System, is a widely-used software tool for energy policy analysis and climate change mitigation assessment. openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.JQ brings cutting edge mobile support to organizations that support mass audiences					
Denial of Service; Overflow	06-May-2016	10	Off-by-one error in the tokenadd function in jv_parse.c in jq allows remote attackers to cause a denial of service (crash) via a long JSON-encoded number, which triggers a heap-based buffer overflow. **Reference:CVE-2015-8863**	https://github.com/stedolan/jq/commit/8eb1367ca44e772963e704a700ef72ae2e12babd	A-JQ -JQ/LE-180516/183
Mcafee/Microsoft					
Virusscan Enterprise/Windows					
McAfee VirusScan Enterprise safeguards systems and files from viruses and other security risks. It detects and removes malware, and configures antivirus policies to manage quarantined items. Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Bypass	05-May-2016	3	The McAfee VirusScan Console (mcconsol.exe) in McAfee VirusScan Enterprise 8.8.0 before Hotfix 1123565 (8.8.0.1546) on Windows allows local administrators to bypass intended self-protection rules and unlock the console window by closing registry handles. **Reference:CVE-2016-4534**	https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26485/en_US/VSE_8_8_HF1123565_release_notes.pdf	A-MCA-VIRUS-180516/184
Canonical;Debian;Fedoraproject/Freedesktop					
Ubuntu Linux/Debian Linux/Fedora/Poppler *Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers. Debian is an operating system and a distribution of Free Software.Poppler is a free software utility library for rendering Portable Document Format (PDF) documents. Fedora /fɪˈdɒr.ə/ (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project*					
Denial of Service; Execute Code; Overflow; Memory Corruption	06-May-2016	9.3	Heap-based buffer overflow in the ExponentialFunction::ExponentialFunction function in Poppler before 0.40.0 allows remote attackers to cause a denial of service (memory corruption and crash) or possibly execute arbitrary code via an invalid blend mode in the ExtGState dictionary in a crafted PDF document. **Reference:CVE-2015-8868**	https://bugs.freedesktop.org/show_bug.cgi?id=93476	A-CAN-UBUNT-180516/185

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Canonical;Fedoraproject/GNU					
Ubuntu Linux/Fedora/Libtasn1 *Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers. Fedora is a Linux based operating system. Libtasn1 is the ASN.1 library used by GnuTLS, GNU Shishi and some other packages.*					
Denial of Service	05-May-2016	4.3	The _asn1_extract_der_octet function in lib/decoding.c in GNU Libtasn1 before 4.8, when used without the ASN1_DECODE_FLAG_STRICT_DER flag, allows remote attackers to cause a denial of service (infinite recursion) via a crafted certificate. **Reference:CVE-2016-4008**	http://git.savannah.gnu.org/gitweb/?p=libtasn1.git;a=commit;h=a6e0a0b58f5cdaf4e9beca5bce69c09808cbb625	A-CAN-UBUNT-180516/186
Debian/Libpam-sshauth					
Debian Linux/Libpam-sshauth *Debian is an operating system and a distribution of Free Software.Libpam-sshauth is a PAM module to authenticate using an SSH server,*					
Gain Previleges; Bypass	06-May-2016	10	The pam_sm_authenticate function in pam_sshauth.c in libpam-sshauth might allow context-dependent attackers to bypass authentication or gain privileges via a system user account. **Reference:CVE-2016-4422**	https://bazaar.launchpad.net/~ltsp-upstream/ltsp/libpam-sshauth/revision/114#src/pam_sshauth.c	A-DEB-DEBIA-180516/187
Debian/Mercurial					
Debian Linux/Mercurial					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Debian is an operating system and a distribution of Free Software. Mercurial is a modern, open source, distributed version control system, and a compelling upgrade from older systems like Subversion.					
Execute Code	09-May-2016	6.8	The convert extension in Mercurial before 3.8 might allow context-dependent attackers to execute arbitrary code via a crafted git repository name. **Reference:CVE-2016-3105**	https://selenic.com/hg/rev/a56296f55a5e	A-DEB-DEBIA-180516/188
Debian/Tardiff Project					
Debian Linux/Tardiff *Debian is an operating system and a distribution of Free Software. Tardiff is a Perl script used to quickly make a tarball of changes between versions of an archive, or between pre- and post-build of an application.*					
NA	06-May-2016	2.1	Cool Projects TarDiff allows local users to write to arbitrary files via a symlink attack on a pathname in a /tmp/tardiff-$$ temporary directory. **Reference:CVE-2015-0858**	https://anonscm.debian.org/cgit/collab-maint/tardiff.git/commit/?id=9bd6a07bc204472ac27242cea16f89943b43003a	A-DEB-DEBIA-180516/189
Execute Code	06-May-2016	10	Cool Projects TarDiff allows remote attackers to execute arbitrary commands via shell metacharacters in the name of a (1) tar file or (2) file within a tar file. **Reference:CVE-2015-0857**	https://anonscm.debian.org/cgit/collab-maint/tardiff.git/commit/?id=9bd6a07bc204472ac27242cea16f89943b43003a	A-DEB-DEBIA-180516/190
Hardware					
Google					

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Android One *Android One is a line of consumer electronics devices that run the Android Operating System.*					
Gain Previleges	09-May-2016	7.6	The MediaTek Wi-Fi driver in Android before 2016-05-01 on Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 27549705. **Reference:CVE-2016-2453**	http://source.android.com/security/bulletin/2016-05-01.html	H-GOO-ANDRO-180516/191
Operating System					
Canonical;Linux					
Ubuntu Core;Ubuntu Linux;Ubuntu Touch/Linux Kernel *Ubuntu Core is the best performing version of Ubuntu for internet-connecteddevices in need of a totally secure, robust and lightweight OS.Ubuntu is an open source software platform.Ubuntu Touch is a mobile version of the Ubuntu operating system developed by Canonical UK Ltd and the Ubuntu community.The Linux kernel is a Unix-like computer operating system kernel*					
Gain Previleges	02-May-2016	7.2	The overlayfs implementation in the Linux kernel through 4.5.2 does not properly restrict the mount namespace, which allows local users to gain privileges by mounting an overlayfs filesystem on top of a FUSE filesystem, and then executing a crafted setuid program. **Reference:CVE-2016-1576**	http://people.canonical.com/~ubuntu-security/cve/2016/CVE-2016-1576.html	O-CAN-UBUNT-180516/192
Gain Previleges	02-May-2016	7.2	The overlayfs implementation in the Linux kernel through	http://people.canonical.com/~ubuntu-	O-CAN-UBUNT-180516/193

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			4.5.2 does not properly maintain POSIX ACL xattr data, which allows local users to gain privileges by leveraging a group-writable setgid directory. **Reference:CVE-2016-1575**	security/cve/2016/CVE-2016-1575.html	
Google					
Android *Android delivers a complete set of software for mobile devices: an operating system, middleware and key mobile applications*					
Denial of Service; Gain Previleges	09-May-2016	4.4	wpa_supplicant 0.4.0 through 2.5 does not reject \n and \r characters in passphrase parameters, which allows local users to trigger arbitrary library loading and consequently gain privileges, or cause a denial of service (daemon outage), via a crafted (1) SET, (2) SET_CRED, or (3) SET_NETWORK command. **Reference:CVE-2016-4477**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/194
NA	09-May-2016	7.6	OpenSSLCipher.java in Conscrypt in Android 6.x before 2016-05-01 mishandles updates of the Additional Authenticated Data	https://android.googlesource.com/platform/external/conscrypt/+/8bec47d2184fca7e8b73	O-GOO-ANDRO-180516/195

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			(AAD) array, which allows attackers to spoof message authentication via unspecified vectors, aka internal bug 27371173. **Reference:CVE-2016-2462**	37d2a65b2b75a9bc8f54	
NA	09-May-2016	7.6	OpenSSLCipher.java in Conscrypt in Android 6.x before 2016-05-01 mishandles resets of the Additional Authenticated Data (AAD) array, which allows attackers to spoof message authentication via unspecified vectors, aka internal bugs 27324690 and 27696681. **Reference:CVE-2016-2461**	https://android.googlesource.com/platform/external/conscrypt/+/1638945d4ed9403790962ec7abed1b7a232a9ff8	O-GOO-ANDRO-180516/196
Gain Information	09-May-2016	4.3	mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not initialize certain data structures, which allows attackers to obtain sensitive information via a crafted application, related to IGraphicBufferConsumer.cpp and	https://android.googlesource.com/platform/frameworks/native/+/a30d7d90c4f718e46fb41a99b3d52800e1011b73	O-GOO-ANDRO-180516/197

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			IGraphicBufferProducer.cpp, aka internal bug 27555981. **Reference:CVE-2016-2460**		
Gain Information	09-May-2016	4.3	mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not initialize certain data structures, which allows attackers to obtain sensitive information via a crafted application, related to IGraphicBufferConsumer.cpp and IGraphicBufferProducer.cpp, aka internal bug 27556038. **Reference:CVE-2016-2459**	https://android.googlesource.com/platform/frameworks/native/+/a30d7d90c4f718e46fb41a99b3d52800e1011b73	O-GOO-ANDRO-180516/198
Gain Information	09-May-2016	4.3	The compose functionality in AOSP Mail in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not properly restrict attachments, which allows attackers to obtain sensitive information via a crafted application, related to ComposeActivity.java and ComposeActivityEmail	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/199

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			.java, aka internal bug 27335139. **Reference:CVE-2016-2458**		
Bypass	09-May-2016	2.1	server/pm/UserManagerService.java in Wi-Fi in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 allows attackers to bypass intended restrictions on Wi-Fi configuration changes by leveraging guest access, aka internal bug 27411179. **Reference:CVE-2016-2457**	https://android.googlesource.com/platform/frameworks/base/+/12332e05f632794e18ea8c4ac52c98e82532e5db	O-GOO-ANDRO-180516/200
Gain Previleges	09-May-2016	6.8	The MediaTek Wi-Fi driver in Android before 2016-05-01 on Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 27275187. **Reference:CVE-2016-2456**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/201
Denial of Service	09-May-2016	7.1	The Qualcomm hardware video codec in Android before 2016-05-01 on Nexus 5 devices allows remote attackers to cause a denial of service (reboot) via a crafted file, aka internal bug 26221024.	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/202

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Reference:CVE-2016-2454		
Gain Previleges	09-May-2016	9.3	codecs/amrnb/dec/SoftAMR.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not validate buffer sizes, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bugs 27662364 and 27843673. **Reference:CVE-2016-2452**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/203
Gain Previleges	09-May-2016	9.3	codecs/on2/dec/SoftVPX.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not validate VPX output buffer sizes, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem	https://android.googlesource.com/platform/frameworks/av/+/f9ed2fe6d61259e779a37d4c2d7edb33a1c1f8ba	O-GOO-ANDRO-180516/204

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			access, aka internal bug 27597103. **Reference:CVE-2016-2451**		
Gain Previleges	09-May-2016	9.3	codecs/on2/enc/SoftVPXEncoder.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not validate OMX buffer sizes, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27569635. **Reference:CVE-2016-2450**	https://android.googlesource.com/platform/frameworks/av/+/7fd96ebfc4c9da496c59d7c45e1f62be178e626d	O-GOO-ANDRO-180516/205
Gain Previleges	09-May-2016	9.3	services/camera/libcameraservice/device3/Camera3Device.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not validate template IDs, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or	https://android.googlesource.com/platform/frameworks/av/+/b04aee833c5cfb6b31b8558350feb14bb1a0f353	O-GOO-ANDRO-180516/206

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			SignatureOrSystem access, aka internal bug 27568958. **Reference:CVE-2016-2449**		
Gain Previleges	09-May-2016	9.3	media/libmediaplayerservice/nuplayer/NuPlayerStreamListener.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not properly validate entry data structures, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27533704. **Reference:CVE-2016-2448**	https://android.googlesource.com/platform/frameworks/av/+/a2d1d85726aa2a3126e9c331a8e00a8c319c9e2b	O-GOO-ANDRO-180516/207
Gain Previleges	09-May-2016	7.6	The NVIDIA media driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27441354. **Reference:CVE-2016-2446**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/208
Gain Previleges	09-May-2016	7.6	The NVIDIA media driver in Android before 2016-05-01 on	http://source.android.com/security/bulleti	O-GOO-ANDRO-180516/209

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27253079. **Reference:CVE-2016-2445**	n/2016-05-01.html	
Gain Previleges	09-May-2016	7.6	The NVIDIA media driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27208332. **Reference:CVE-2016-2444**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/210
Gain Previleges	09-May-2016	7.6	The Qualcomm MDP driver in Android before 2016-05-01 on Nexus 5 and Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 26404525. **Reference:CVE-2016-2443**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/211
Gain Previleges	09-May-2016	7.6	The Qualcomm buspm driver in Android before 2016-05-01 on Nexus 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 26494907.	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/212

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Reference:CVE-2016-2442		
Gain Previleges	09-May-2016	7.6	The Qualcomm buspm driver in Android before 2016-05-01 on Nexus 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 26354602. **Reference:CVE-2016-2441**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/213
Gain Previleges	09-May-2016	9.3	libs/binder/IPCThreadState.cpp in Binder in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 mishandles object references, which allows attackers to gain privileges via a crafted application, aka internal bug 27252896. **Reference:CVE-2016-2440**	https://android.googlesource.com/platform/frameworks/native/+/a59b827869a2ea04022dd225007f29af8d61837a	O-GOO-ANDRO-180516/214
Execute Code; Overflow	09-May-2016	5.4	Buffer overflow in btif/src/btif_dm.c in Bluetooth in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 allows remote attackers to execute arbitrary code via a long PIN value, aka	https://android.googlesource.com/platform/system/bt/+/9b534de2aca5d790c2a1c4d76b545f16137d95dd	O-GOO-ANDRO-180516/215

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			internal bug 27411268. **Reference:CVE-2016-2439**		
Gain Previleges	09-May-2016	9.3	The NVIDIA video driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27436822. **Reference:CVE-2016-2437**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/216
Gain Previleges	09-May-2016	9.3	The NVIDIA video driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27299111. **Reference:CVE-2016-2436**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/217
Gain Previleges	09-May-2016	9.3	The NVIDIA video driver in Android before 2016-05-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27297988. **Reference:CVE-2016-2435**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/218
Gain Previleges	09-May-2016	9.3	The NVIDIA video driver in Android before 2016-05-01 on Nexus 9 devices	http://source.android.com/security/bulletin/2016-05-	O-GOO-ANDRO-180516/219

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			allows attackers to gain privileges via a crafted application, aka internal bug 27251090. **Reference:CVE-2016-2434**	01.html	
Gain Previleges	09-May-2016	9.3	The Qualcomm TrustZone component in Android before 2016-05-01 on Nexus 6 and Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 25913059. **Reference:CVE-2016-2432**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/220
Gain Previleges	09-May-2016	9.3	The Qualcomm TrustZone component in Android before 2016-05-01 on Nexus 5, Nexus 6, Nexus 7 (2013), and Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 24968809. **Reference:CVE-2016-2431**	http://source.android.com/security/bulletin/2016-05-01.html	O-GOO-ANDRO-180516/221
Gain Previleges	09-May-2016	9.3	libbacktrace/Backtrace.cpp in debuggerd in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 allows	https://android.googlesource.com/platform/system/core/ +/ad54cfed4516292654c99	O-GOO-ANDRO-180516/222

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			attackers to gain privileges via an application containing a crafted symbol name, aka internal bug 27299236. **Reference:CVE-2016-2430**	7910839153264ae00a0	
Denial of Service; Execute Code; Overflow; Memory Corruption	09-May-2016	10	libFLAC/stream_decoder.c in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not prevent free operations on uninitialized memory, which allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted media file, aka internal bug 27211885. **Reference:CVE-2016-2429**	https://android.googlesource.com/platform/external/flac/+/b499389da21d89d32deff500376c5ee4f8f0b04c	O-GOO-ANDRO-180516/223
Denial of Service; Execute Code; Overflow; Memory Corruption	09-May-2016	10	libAACdec/src/aacdec_drc.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not properly limit the number of threads, which allows remote attackers to execute	https://android.googlesource.com/platform/external/aac/+/5d4405f601fa11a8955fd7611532c982420e4206	O-GOO-ANDRO-180516/224

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			arbitrary code or cause a denial of service (stack memory corruption) via a crafted media file, aka internal bug 26751339. **Reference:CVE-2016-2428**		
Linux					
Linux Kernel *The Linux kernel is a Unix-like computer operating system kernel*					
Denial of Service	02-May-2016	4.9	Double free vulnerability in drivers/net/usb/cdc_ncm.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (system crash) or possibly have unspecified other impact by inserting a USB device with an invalid USB descriptor. **Reference:CVE-2016-3951**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=4d06dd537f95683aba3651098ae288b7cbff8274	O-LIN-LINUX-180516/225
Denial of Service	02-May-2016	4.9	The ims_pcu_parse_cdc_data function in drivers/input/misc/ims-pcu.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (system crash) via a USB device without both a	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=a0ad220c96692eda76b2e3fd7279f3dcd1d8a8ff	O-LIN-LINUX-180516/226

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			master and a slave interface. **Reference:CVE-2016-3689**		
Denial of Service	02-May-2016	4.9	The digi_port_init function in drivers/usb/serial/digi_acceleport.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor. **Reference:CVE-2016-3140**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=5a07975ad0a36708c6b0a5b9fea1ff811d0b0c1f	O-LIN-LINUX-180516/227
Denial of Service	02-May-2016	4.9	The acm_probe function in drivers/usb/class/cdc-acm.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without both a control and a data endpoint descriptor. **Reference:CVE-2016-3138**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8835ba4a39cf53f705417b3b3a94eb067673f2c9	O-LIN-LINUX-180516/228
Denial of Service	02-May-2016	4.9	drivers/usb/serial/cypress_m8.c in the Linux kernel before 4.5.1 allows physically	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-	O-LIN-LINUX-180516/229

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without both an interrupt-in and an interrupt-out endpoint descriptor, related to the cypress_generic_port_probe and cypress_open functions. **Reference:CVE-2016-3137**	4.5.1	
Denial of Service	02-May-2016	4.9	The mct_u232_msr_to_state function in drivers/usb/serial/mct_u232.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device without two interrupt-in endpoint descriptors. **Reference:CVE-2016-3136**	https://bugzilla.redhat.com/show_bug.cgi?id=1317007	O-LIN-LINUX-180516/230
Gain Previleges	02-May-2016	4.6	The aufs module for the Linux kernel 3.x and 4.x does not properly maintain POSIX ACL xattr data, which allows local users to gain		O-LIN-LINUX-180516/231

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			privileges by leveraging a group-writable setgid directory. **Reference:CVE-2016-2854**		
Gain Previleges	02-May-2016	4.4	The aufs module for the Linux kernel 3.x and 4.x does not properly restrict the mount namespace, which allows local users to gain privileges by mounting an aufs filesystem on top of a FUSE filesystem, and then executing a crafted setuid program. **Reference:CVE-2016-2853**		O-LIN-LINUX-180516/232
Denial of Service	02-May-2016	4.9	The iowarrior_probe function in drivers/usb/misc/iowarrior.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor. **Reference:CVE-2016-2188**	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.1	O-LIN-LINUX-180516/233
Denial of Service	02-May-2016	4.9	The gtco_probe function in drivers/input/tablet/gt	http://git.kernel.org/cgit/linux/kernel/git/t	O-LIN-LINUX-180516/234

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			co.c in the Linux kernel through 4.5.2 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor. **Reference:CVE-2016-2187**	orvalds/linux.git/commit/?id=162f98dea487206d9ab79fc12ed64700667a894d	
Denial of Service	02-May-2016	4.9	The powermate_probe function in drivers/input/misc/powermate.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor. **Reference:CVE-2016-2186**	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.1	O-LIN-LINUX-180516/235
Denial of Service	02-May-2016	4.9	The ati_remote2_probe function in drivers/input/misc/ati_remote2.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a	https://github.com/torvalds/linux/commit/950336ba3e4a1ffd2ca60d29f6ef386dd2c7351d	O-LIN-LINUX-180516/236

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			crafted endpoints value in a USB device descriptor. **Reference:CVE-2016-2185**		
Gain Information	02-May-2016	5	The atl2_probe function in drivers/net/ethernet/atheros/atlx/atl2.c in the Linux kernel through 4.5.2 incorrectly enables scatter/gather I/O, which allows remote attackers to obtain sensitive information from kernel memory by reading packet data. **Reference:CVE-2016-2117**	https://github.com/torvalds/linux/commit/f43bfaeddc79effbf3d0fcb53ca477cca66f3db8	O-LIN-LINUX-180516/237
Denial of Service	02-May-2016	7.8	The tcp_cwnd_reduction function in net/ipv4/tcp_input.c in the Linux kernel before 4.3.5 allows remote attackers to cause a denial of service (divide-by-zero error and system crash) via crafted TCP traffic. **Reference:CVE-2016-2070**	https://github.com/torvalds/linux/commit/8b8a321ff72c785ed5e8b4cf6eda20b35d427390	O-LIN-LINUX-180516/238
Denial of Service; Overflow	05-May-2016	7.2	The adreno_perfcounter_query_group function in drivers/gpu/msm/adreno_perfcounter.c in	https://www.codeaurora.org/buffer-overflow-adreno-gpu-msm-driver-	O-LIN-LINUX-180516/239

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			the Adreno GPU driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, uses an incorrect integer data type, which allows attackers to cause a denial of service (integer overflow, heap-based buffer overflow, and incorrect memory allocation) or possibly have unspecified other impact via a crafted IOCTL_KGSL_PERFCOUNTER_QUERY ioctl call. **Reference:CVE-2016-2062**	cve-2016-2062	
Denial of Service; Gain Previleges	05-May-2016	7.2	The msm_ipc_router_bind_control_port function in net/ipc_router/ipc_router_core.c in the IPC router kernel module for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not verify that a port is a client port, which	https://www.codeaurora.org/projects/security-advisories/linux-ipc-router-binding-any-port-control-port-cve-2016-2059	O-LIN-LINUX-180516/240

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			allows attackers to gain privileges or cause a denial of service (race condition and list corruption) by making many BIND_CONTROL_PORT ioctl calls. **Reference:CVE-2016-2059**		
Denial of Service	02-May-2016	7.1	The asn1_ber_decoder function in lib/asn1_decoder.c in the Linux kernel before 4.3 allows attackers to cause a denial of service (panic) via an ASN.1 BER file that lacks a public key, leading to mishandling by the public_key_verify_signature function in crypto/asymmetric_keys/public_key.c. **Reference:CVE-2016-2053**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=0d62e9dd6da45bbf0f33a8617afc5fe774c8f45f	O-LIN-LINUX-180516/241
Denial of Service	02-May-2016	1.9	Multiple race conditions in the ext4 filesystem implementation in the Linux kernel before 4.5 allow local users to cause a denial of service (disk corruption) by writing to a page that is associated with a different user's file	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=ea3d7209ca01da209cda6f0dea8be9cc4b7a933b	O-LIN-LINUX-180516/242

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			after unsynchronized hole punching and page-fault handling. **Reference:CVE-2015-8839**		
Denial of Service; Overflow	02-May-2016	7.2	Integer overflow in the aio_setup_single_vector function in fs/aio.c in the Linux kernel 4.0 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. NOTE: this vulnerability exists because of a CVE-2012-6701 regression. **Reference:CVE-2015-8830**	https://github.com/torvalds/linux/commit/c4f4b82694fe48b02f7a881a1797131a6dad1364	O-LIN-LINUX-180516/243
Denial of Service	02-May-2016	5	fs/nfs/nfs4proc.c in the NFS client in the Linux kernel before 4.2.2 does not properly initialize memory for migration recovery operations, which allows remote NFS servers to cause a denial of service (NULL pointer dereference and panic) via crafted network traffic. **Reference:CVE-2015-8746**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=18e3b739fdc826481c6a1335ce0c5b19b3d415da	O-LIN-LINUX-180516/244
Denial of Service	02-May-2016	4.9	The ext4 implementation in the	https://github.com/torvalds/l	O-LIN-LINUX-180516/245

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Linux kernel before 2.6.34 does not properly track the initialization of certain data structures, which allows physically proximate attackers to cause a denial of service (NULL pointer dereference and panic) via a crafted USB device, related to the ext4_fill_super function. **Reference:CVE-2015-8324**	inux/commit/744692dc059845b2a3022119871846e74d4f6e11	
Denial of Service; Memory Corruption	02-May-2016	7.2	The skb_copy_and_csum_datagram_iovec function in net/core/datagram.c in the Linux kernel 3.14.54 and 3.18.22 does not accept a length argument, which allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact via a write system call followed by a recvmsg system call. **Reference:CVE-2015-8019**	https://bugzilla.redhat.com/show_bug.cgi?id=1276588	O-LIN-LINUX-180516/246
Denial of Service	02-May-2016	4.9	The fs_pin implementation in the Linux kernel before 4.0.5 does not ensure	https://github.com/torvalds/linux/commit/820f9f147dcc	O-LIN-LINUX-180516/247

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			the internal consistency of a certain list data structure, which allows local users to cause a denial of service (system crash) by leveraging user-namespace root access for an MNT_DETACH umount2 system call, related to fs/fs_pin.c and include/linux/fs_pin.h. **Reference:CVE-2015-4178**	e2602eefd9b575bbbd9ea14f0953	
Denial of Service	02-May-2016	4.9	The collect_mounts function in fs/namespace.c in the Linux kernel before 4.0.5 does not properly consider that it may execute after a path has been unmounted, which allows local users to cause a denial of service (system crash) by leveraging user-namespace root access for an MNT_DETACH umount2 system call. **Reference:CVE-2015-4177**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=cd4a40174b71acd021877341684d8bb1dc8ea4ae	O-LIN-LINUX-180516/248
Gain Information	02-May-2016	2.1	fs/namespace.c in the Linux kernel before 4.0.2 does not properly support mount connectivity,	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?	O-LIN-LINUX-180516/249

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			which allows local users to read arbitrary files by leveraging user-namespace root access for deletion of a file or directory. **Reference:CVE-2015-4176**	id=e0c9c0afd2fc958ffa34b697972721d81df8a56f	
Denial of Service	02-May-2016	4.7	Race condition in the ldsem_cmpxchg function in drivers/tty/tty_ldsem.c in the Linux kernel before 3.13-rc4-next-20131218 allows local users to cause a denial of service (ldsem_down_read and ldsem_down_write deadlock) by establishing a new tty thread during shutdown of a previous tty thread. **Reference:CVE-2015-4170**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=cf872776fc84128bb779ce2b83a37c884c3203ae	O-LIN-LINUX-180516/250
Gain Previleges	02-May-2016	7.2	net/socket.c in the Linux kernel 3.19 before 3.19.3 does not validate certain range data for (1) sendto and (2) recvfrom system calls, which allows local users to gain privileges by leveraging a subsystem that uses the copy_from_iter function in the iov_iter	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=4de930efc23b92ddf88ce91c405ee645fe6e27ea	O-LIN-LINUX-180516/251

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			interface, as demonstrated by the Bluetooth subsystem. **Reference:CVE-2015-2686**		
Denial of Service	02-May-2016	4.9	The xsave/xrstor implementation in arch/x86/include/asm/xsave.h in the Linux kernel before 3.19.2 creates certain .altinstr_replacement pointers and consequently does not provide any protection against instruction faulting, which allows local users to cause a denial of service (panic) by triggering a fault, as demonstrated by an unaligned memory operand or a non-canonical address memory operand. **Reference:CVE-2015-2672**	http://www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.19.2	O-LIN-LINUX-180516/252
Denial of Service	02-May-2016	4.9	The nft_flush_table function in net/netfilter/nf_tables_api.c in the Linux kernel before 3.18.5 mishandles the interaction between cross-chain jumps and ruleset flushes, which allows local users to cause a denial of service (panic) by	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=a2f18db0c68fec96631c10cad9384c196e9008ac	O-LIN-LINUX-180516/253

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			leveraging the CAP_NET_ADMIN capability. **Reference:CVE-2015-1573**		
Denial of Service	02-May-2016	2.1	The VFS subsystem in the Linux kernel 3.x provides an incomplete set of requirements for setattr operations that underspecifies removing extended privilege attributes, which allows local users to cause a denial of service (capability stripping) via a failed invocation of a system call, as demonstrated by using chown to remove a capability from the ping or Wireshark dumpcap program. **Reference:CVE-2015-1350**	https://bugzilla.redhat.com/show_bug.cgi?id=1185139	O-LIN-LINUX-180516/254
Gain Previleges	09-May-2016	9.3	The WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not verify authorization for private SET IOCTL calls, which allows attackers to gain	http://source.android.com/security/bulletin/2016-05-01.html	O-LIN-LINUX-180516/255

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			privileges via a crafted application, related to wlan_hdd_hostapd.c and wlan_hdd_wext.c. **CVE-2015-0571**		
Overflow; Gain Previleges	09-May-2016	9.3	Stack-based buffer overflow in the SET_WPS_IE IOCTL implementation in wlan_hdd_hostapd.c in the WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges via a crafted application that uses a long WPS IE element. **Reference:CVE-2015-0570**	https://www.codeaurora.org/projects/security-advisories/multiple-issues-wlan-driver-allow-local-privilege-escalation-cve-2015	O-LIN-LINUX-180516/256
Overflow; Gain Previleges	09-May-2016	9.3	Heap-based buffer overflow in the private wireless extensions IOCTL implementation in wlan_hdd_wext.c in the WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other	http://source.android.com/security/bulletin/2016-05-01.html	O-LIN-LINUX-180516/257

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			products, allows attackers to gain privileges via a crafted application that establishes a packet filter. **Reference:CVE-2015-0569**		
Bypass	02-May-2016	3.6	fs/namespace.c in the Linux kernel before 4.0.2 processes MNT_DETACH umount2 system calls without verifying that the MNT_LOCKED flag is unset, which allows local users to bypass intended access restrictions and navigate to filesystem locations beneath a mount by calling umount2 within a user namespace. **Reference:CVE-2014-9717**	https://bugzilla.redhat.com/show_bug.cgi?id=1226751	O-LIN-LINUX-180516/258
Denial of Service; Overflow	02-May-2016	7.2	Integer overflow in fs/aio.c in the Linux kernel before 3.4.1 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. **Reference:CVE-2012-6701**	http://www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.4.1	O-LIN-LINUX-180516/259
NA	02-May-2016	7.2	The netlink_sendmsg function in net/netlink/af_netlink.c in the Linux kernel	https://github.com/torvalds/linux/commit/20e1db19db5	O-LIN-LINUX-180516/260

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			before 3.5.5 does not validate the dst_pid field, which allows local users to have an unspecified impact by spoofing Netlink messages. **Reference:CVE-2012-6689**	d6b9e4e83021595eab0dc8f107bef	
Denial of Service	02-May-2016	4.9	The tty_open function in drivers/tty/tty_io.c in the Linux kernel before 3.1.1 mishandles a driver-lookup failure, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via crafted access to a device file under the /dev/pts directory. **Reference:CVE-2011-5321**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c290f8358acaeffd8e0c551ddcc24d1206143376	O-LIN-LINUX-180516/261
Denial of Service	02-May-2016	2.1	mm/filemap.c in the Linux kernel before 2.6.25 allows local users to cause a denial of service (infinite loop) via a writev system call that triggers an iovec of zero length, followed by a page fault for an iovec of nonzero length. **Reference:CVE-**	http://mirror.linux.org.au/linux/kernel/v2.6/ChangeLog-2.6.25	O-LIN-LINUX-180516/262

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			2008-7316		
Denial of Service	02-May-2016	7.8	The redirect_target function in net/ipv4/netfilter/ipt_REDIRECT.c in the Linux kernel before 2.6.0 allows remote attackers to cause a denial of service (NULL pointer dereference and OOPS) by sending packets to an interface that has a 0.0.0.0 IP address, a related issue to CVE-2015-8787. **Reference:CVE-2003-1604**	https://bugzilla.redhat.com/show_bug.cgi?id=1303072	O-LIN-LINUX-180516/263
Microsoft					
Windows 10					
Microsoft Windows (or simply Windows) is a metafamily of graphical operating systemsdeveloped, 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.					
Bypass	10-May-2016	2.1	Microsoft Windows 10 Gold and 1511 allows local users to bypass the Virtual Secure Mode Hypervisor Code Integrity (HVCI) protection mechanism and perform RWX markings of kernel-mode pages via a crafted application, aka "Hypervisor Code Integrity Security Feature Bypass." **Reference:CVE-2016-0181**	http://technet.microsoft.com/en-us/security/bulletin/ms16-066	O-MIC-WINDO-180516/264

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
Gain Previleges	10-May-2016	7.2	dxgkrnl.sys in the DirectX Graphics kernel subsystem in the kernel-mode drivers in Microsoft Windows 7 SP1, Windows Server 2008 R2 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 "Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability." **Reference:CVE-2016-0176**	http://technet.microsoft.com/en-us/security/bulletin/ms16-062	O-MIC-WINDO-180516/265
Gain Previleges	10-May-2016	7.2	dxgkrnl.sys in the DirectX Graphics kernel subsystem in the kernel-mode drivers 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 "Microsoft DirectX Graphics Kernel	http://technet.microsoft.com/en-us/security/bulletin/ms16-062	O-MIC-WINDO-180516/266

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Subsystem Elevation of Privilege Vulnerability." **Reference:CVE-2016-0197**		
Gain Previleges	10-May-2016	7.2	The kernel-mode drivers 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 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0171, CVE-2016-0173, and CVE-2016-0174. **Reference:CVE-2016-0196**	http://technet.microsoft.com/en-us/security/bulletin/ms16-062	O-MIC-WINDO-180516/267
Execute Code; Overflow; Memory Corruption	10-May-2016	9.3	The Imaging Component 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	http://technet.microsoft.com/en-us/security/bulletin/ms16-055	O-MIC-WINDO-180516/268

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			arbitrary code via a crafted document, aka "Windows Imaging Component Memory Corruption Vulnerability." **Reference:CVE-2016-0195**		
Execute Code	10-May-2016	9.3	Use-after-free vulnerability in GDI 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 document, aka "Direct3D Use After Free Vulnerability." **Reference:CVE-2016-0184**	http://technet.microsoft.com/en-us/security/bulletin/ms16-055	O-MIC-WINDO-180516/269
Gain Previleges	10-May-2016	7.2	The kernel 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 mishandles symbolic links, which allows local users to gain	http://technet.microsoft.com/en-us/security/bulletin/ms16-060	O-MIC-WINDO-180516/270

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			privileges via a crafted application, aka "Windows Kernel Elevation of Privilege Vulnerability." **Reference:CVE-2016-0180**		
Execute Code	10-May-2016	9	The RPC NDR Engine 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 mishandles free operations, which allows remote attackers to execute arbitrary code via malformed RPC requests, aka "RPC Network Data Representation Engine Elevation of Privilege Vulnerability." **Reference:CVE-2016-0178**	http://technet.microsoft.com/en-us/security/bulletin/ms16-061	O-MIC-WINDO-180516/271
Bypass; Gain Information	10-May-2016	2.1	The kernel-mode drivers 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	http://technet.microsoft.com/en-us/security/bulletin/ms16-062	O-MIC-WINDO-180516/272

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			10 Gold and 1511 allow local users to obtain sensitive information about kernel-object addresses, and consequently bypass the KASLR protection mechanism, via a crafted application, aka "Win32k Information Disclosure Vulnerability." **Reference:CVE-2016-0175**		
Gain Previleges	10-May-2016	7.2	The kernel-mode drivers 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 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0171, CVE-2016-0173, and CVE-2016-0196. **Reference:CVE-2016-0174**	http://technet.microsoft.com/en-us/security/bulletin/ms16-062	O-MIC-WINDO-180516/273
Gain Previleges	10-May-2016	7.2	The kernel-mode drivers in Microsoft Windows Vista SP2,	http://technet.microsoft.com/en-	O-MIC-WINDO-180516/274

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			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 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0171, CVE-2016-0174, and CVE-2016-0196. **Reference:CVE-2016-0173**	us/security/bulletin/ms16-062	
Gain Previleges	10-May-2016	7.2	The kernel-mode drivers 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 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0173, CVE-2016-0174, and CVE-2016-0196.	http://technet.microsoft.com/en-us/security/bulletin/ms16-062	O-MIC-WINDO-180516/275

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			Reference:CVE-2016-0171		
Execute Code	10-May-2016	9.3	GDI 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 document, aka "Windows Graphics Component RCE Vulnerability." **Reference:CVE-2016-0170**	http://technet.microsoft.com/en-us/security/bulletin/ms16-055	O-MIC-WINDO-180516/276
Gain Information	10-May-2016	4.3	GDI 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 obtain sensitive information via a crafted document, aka "Windows Graphics Component Information Disclosure Vulnerability," a different vulnerability	http://technet.microsoft.com/en-us/security/bulletin/ms16-055	O-MIC-WINDO-180516/277

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			than CVE-2016-0168. **Reference:CVE-2016-0169**		
Gain Information	10-May-2016	4.3	GDI 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 obtain sensitive information via a crafted document, aka "Windows Graphics Component Information Disclosure Vulnerability," a different vulnerability than CVE-2016-0169. **Reference:CVE-2016-0168**	http://technet.microsoft.com/en-us/security/bulletin/ms16-055	O-MIC-WINDO-180516/278
Execute Code; Memory Corruption	10-May-2016	9.3	Windows Journal in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted Journal (aka .jnt) file, aka "Windows Journal Memory Corruption Vulnerability." **Reference:CVE-**	http://technet.microsoft.com/en-us/security/bulletin/ms16-056	O-MIC-WINDO-180516/279

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			2016-0182		
Execute Code	10-May-2016	9.3	Windows Shell in Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted web site, aka "Windows Shell Remote Code Execution Vulnerability." **Reference:CVE-2016-0179**	http://technet.microsoft.com/en-us/security/bulletin/ms16-057	O-MIC-WINDO-180516/280
Execute Code	10-May-2016	9.3	Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, and Windows 8.1 allows remote attackers to execute arbitrary code via a crafted Media Center link (aka .mcl) file, aka "Windows Media Center Remote Code Execution Vulnerability." **Reference:CVE-2016-0185**	http://technet.microsoft.com/en-us/security/bulletin/ms16-059	O-MIC-WINDO-180516/281
Gain Information	10-May-2016	2.1	Volume Manager Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 does not properly check whether RemoteFX RDP USB disk	http://technet.microsoft.com/en-us/security/bulletin/ms16-067	O-MIC-WINDO-180516/282

Product/ Vulnerability Type(s)	Publish Date	CVSS	Vulnerability Description	Patch (if any)	NCIIPC ID
			accesses originate from the user who mounted a disk, which allows local users to read arbitrary files on these disks via RemoteFX requests, aka "Remote Desktop Protocol Drive Redirection Information Disclosure Vulnerability." **Reference:CVE-2016-0190**		
Execute Code; Gain Previleges	10-May-2016	7.2	Internet Information Services (IIS) in Microsoft Windows Vista SP2 and Server 2008 SP2 mishandles library loading, which allows local users to gain privileges via a crafted application, aka "Windows DLL Loading Remote Code Execution Vulnerability." **Reference:CVE-2016-0152**	http://technet.microsoft.com/en-us/security/bulletin/ms16-058	O-MIC-WINDO-180516/283