National Critical Information Infrastructure Protection Centre

CVE Report

16th Aug – 15th Sept 2016 **Vol. 03 No. 15**

Vulnerability Type(s)	Publish Date	CVSS	Description	Patch	NCIIPC ID
Application(A)					
Accellion					
Kiteworks Appliance *Kiteworks Appliance by Accellion is a secure file sharing platform that facilitates access to enterprise content sources by allowing internal and external users to share, send, sync and edit files on any type of device from any content store*					
Directory Traversal	2016-08-26	5	Directory traversal vulnerability on Accellion Kiteworks appliances before kw2016.03.00 allows remote attackers to read files via a crafted URI. **Reference: CVE-2016-5664**	http://www.kb.cert.org/vuls/id/305607	A-ACC-KITEW-210916/01
Cross-site scripting	2016-08-26	4.3	Multiple cross-site scripting (Cross-site scripting) vulnerabilities in oauth_callback.php on Accellion Kiteworks appliances before kw2016.03.00 allow remote attackers to inject arbitrary web script or HTML via the (1) code, (2) error, or (3) error_description parameter. **Reference: CVE-2016-5663**	http://www.kb.cert.org/vuls/id/305607	A-ACC-KITEW-210916/02
Gain Privileges	2016-08-26	7.2	Accellion Kiteworks appliances before kw2016.03.00 use setuid-root permissions for /opt/bin/cli, which allows local users to gain privileges via unspecified vectors.	http://www.kb.cert.org/vuls/id/305607	A-ACC-KITEW-210916/03

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

		🟧	**Reference: CVE-2016-5662**		
Adobe					
Acrobat; Acrobat Dc; Acrobat Reader Dc; Reader *Use Acrobat to convert, edit and sign PDF files at your desk or on the go. Adobe Acrobat DC is a trusted PDF creator. Adobe Acrobat Reader DC software is the free global standard for reliably viewing, printing, and commenting on PDF documents. Adobe Reader is the most popular program in the world for viewing, creating, managing and manipulating PDF (Portable Document Format) files.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-26	10	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-ACROB-210916/04

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

			2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, and CVE-2016-4269. **Reference: CVE-2016-4270**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-26	10	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, and CVE-2016-4270.	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-ACROB-210916/05

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

			Reference: CVE-2016-4269		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-26	10	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4269, and CVE-2016-4270. **Reference: CVE-2016-**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-ACROB-210916/06

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

			4268		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-26	10	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270. **Reference: CVE-2016-**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-ACROB-210916/07

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

			4267		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-26	10	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4267, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270. **Reference: CVE-2016-4266**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-ACROB-210916/08

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

Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-26	10	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270. **Reference: CVE-2016-4265**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-ACROB-210916/09

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

Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-26	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, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-	https://helpx.adobe.com/security/products/acrobat/apsb16-14.html	A-ADO-ACROB-210916/10

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

			4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105. **Reference: CVE-2016-4119**		
Coldfusion *Adobe ColdFusion is a tried and tested application server that simplifies complex coding tasks.*					
NA	2016-09-01	6.4	The Office Open XML (OOXML) feature in Adobe ColdFusion 10 before Update 21 and 11 before Update 10 allows remote attackers to read arbitrary files or send TCP requests to intranet servers via a crafted OOXML spreadsheet containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. **Reference: CVE-2016-4264**	https://helpx.adobe.com/security/products/coldfusion/apsb16-30.html	A-ADO-COLDF-210916/11
Flash Player *Adobe Flash Player is freeware software for using content created on the Adobe Flash platform, including viewing multimedia, executing rich Internet applications, and streaming video and audio*					
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/12

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

			than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, and CVE-2016-6931. **Reference: CVE-2016-6932**		
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, and CVE-2016-6932. **Reference: CVE-2016-6931**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/13
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/14

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

			than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6931, and CVE-2016-6932. **Reference: CVE-2016-6930**		
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932. **Reference: CVE-2016-6929**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/15
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/16

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

			than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932. **Reference: CVE-2016-6927**		
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932. **Reference: CVE-2016-6926**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/17
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/18

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

			than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932. **Reference: CVE-2016-6925**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, and CVE-2016-6922. **Reference: CVE-2016-6924**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/19
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/20

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

			than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932. **Reference: CVE-2016-6923**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, and CVE-2016-6924. **Reference: CVE-2016-6922**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/21
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/22

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

			than CVE-2016-4272, CVE-2016-4279, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932. **Reference: CVE-2016-6921**		
Execute Code; Memory Overflow	2016-09-14	10	Integer overflow in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-4287**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/23
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-6922, and CVE-2016-6924. **Reference: CVE-2016-4285**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/24

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

Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924. **Reference: CVE-2016-4284**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/25
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924. **Reference: CVE-2016-4283**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/26

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

Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924. **Reference: CVE-2016-4282**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/27
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924. **Reference: CVE-2016-4281**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/28

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

Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924. **Reference: CVE-2016-4280**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/29
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932. **Reference: CVE-2016-4279**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/30

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

Bypass; Gain Information	2016-09-14	5	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-4271 and CVE-2016-4277. **Reference: CVE-2016-4278**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/31
Bypass; Gain Information	2016-09-14	5	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-4271 and CVE-2016-4278. **Reference: CVE-2016-4277**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/32
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/33

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

			than CVE-2016-4274, CVE-2016-4275, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924. **Reference: CVE-2016-4276**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924. **Reference: CVE-2016-4275**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/34
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	10	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/35

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

			than CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924. **Reference: CVE-2016-4274**		
Execute Code	2016-09-14	10	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932. **Reference: CVE-2016-4272**	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/36
Bypass; Gain Information	2016-09-14	5	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-210916/37

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

			than CVE-2016-4277 and CVE-2016-4278. **Reference: CVE-2016-4271**		
Akabei Soft2					
Visual Novel Database *Akabeisoft2 is a Japanese visual novel producing company emerged from the former doujin circle Akabei Soft.*					
Execute Code	2016-09-01	6.8	AKABEi SOFT2 games allow remote attackers to execute arbitrary OS commands via crafted saved data, as demonstrated by Happy Wardrobe. **Reference: CVE-2016-4853**	http://jvn.jp/en/jp/JVN85213412/995740/index.html	A-AKA-VISUA-210916/38
Aki-null					
Yorufukurou: *NA*					
Denial of Service	2016-09-12	4.3	YoruFukurou (NightOwl) before 2.85 relies on support for emoji skin-tone modifiers even though this support is missing from the CoreText CTFramesetter API on OS X 10.9, which allows remote attackers to cause a denial of service (application crash) via a crafted emoji character sequence. **Reference: CVE-2016-4852**	http://jvn.jp/en/jp/JVN94816361/995844/index.html	A-AKI-YORUF-210916/39
Apache					
Openmeetings *Openmeetings provides video conferencing, instant messaging, white board, collaborative document editing and other groupware tools using API functions of the Red5 Streaming Server for Remoting and Streaming.*					

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

Cross-site scripting	2016-08-19	4.3	Cross-site scripting (XSS) vulnerability in the SWF panel in Apache OpenMeetings before 3.1.2 allows remote attackers to inject arbitrary web script or HTML via the swf parameter. **Reference: CVE-2016-3089**	http://openmeetings.apache.org/security.html	A-APA-OPENM-210916/40
Sentry *Apache Sentry is a system for enforcing fine grained role based authorization to data and metadata stored on a hadoop cluster.*					
Execute Code	2016-08-19	6.5	Multiple incomplete blacklist vulnerabilities in Apache Sentry before 1.7.0 allow remote authenticated users to execute arbitrary code via the (1) reflect, (2) reflect2, or (3) java_method Hive builtin functions. **Reference: CVE-2016-0760**	NA	A-APA-SENTR-210916/41
Apple; Google; Microsoft; Mozilla; Opera					
Safari/Chrome/Edge; Internet Explorer/Firefox/Opera *Safari / Chrome / Edge / Internet Explorer / Firefox / Opera are browsers (a browser is an application program that provides a way to look at and interact with all the information on the World Wide Web).*					
Gain Information	2016-09-06	5	The HTTP/2 protocol does not consider the role of the TCP congestion window in providing information about content length, which makes it easier for remote attackers to obtain cleartext data by leveraging a web-browser configuration in which third-party cookies are sent, aka a "HEIST"	NA	A-APP-SAFAR-210916/42

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

			attack. **Reference: CVE-2016-7153**		
Gain Information	2016-09-06	5	The HTTPS protocol does not consider the role of the TCP congestion window in providing information about content length, which makes it easier for remote attackers to obtain cleartext data by leveraging a web-browser configuration in which third-party cookies are sent, aka a "HEIST" attack. **Reference: CVE-2016-7152**	NA	A-APP-SAFAR-210916/43
Cisco					
Adaptive Security Appliance Software *Cisco ASA Software delivers enterprise-class security capabilities for the ASA security family in a variety of form factors.*					
Gain Privileges	2016-08-18	6.8	Cisco Adaptive Security Appliance (ASA) Software before 8.4(1) on ASA 5500, ASA 5500-X, PIX, and FWSM devices allows local users to gain privileges via invalid CLI commands, aka Bug ID CSCtu74257 or EPICBANANA. **Reference: CVE-2016-6367**	http://tools.cisco.com/security/center/viewErp.x?alertId=ERP-56516	A-CIS-ADAPT-210916/44
Aironet Access Point Software: *NA*					
Denial of Service; Memory Overflow	2016-08-22	6.1	The rate-limit feature in the 802.11 protocol implementation on Cisco Aironet 1800, 2800, and 3800 devices with software before 8.2.121.0 and 8.3.x before 8.3.102.0 allows remote	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-AIRON-210916/45

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

			attackers to cause a denial of service (device reload) via crafted 802.11 frames, aka Bug ID CSCva06192. **Reference: CVE-2016-6363**	20160817-aap2	
Gain Privileges	2016-08-22	7.2	Cisco Aironet 1800, 2800, and 3800 devices with software before 8.2.110.0, 8.2.12x before 8.2.121.0, and 8.3.x before 8.3.102.0 allow local users to gain privileges via crafted CLI parameters, aka Bug ID CSCuz24725. **Reference: CVE-2016-6362**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap1	A-CIS-AIRON-210916/46
Denial of Service	2016-08-22	6.1	The Aggregated MAC Protocol Data Unit (AMPDU) implementation on Cisco Aironet 1800, 2800, and 3800 devices with software before 8.2.121.0 and 8.3.x before 8.3.102.0 allows remote attackers to cause a denial of service (device reload) via a crafted AMPDU header, aka Bug ID CSCuz56288. **Reference: CVE-2016-6361**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap	A-CIS-AIRON-210916/47
Anyconnect Secure Mobility Client *This software is used to give any user highly secure access to the enterprise network, from any device, at any time, in any location and to gain more insight into user and endpoint behavior with full visibility across the extended enterprise*					
Gain Privileges	2016-08-25	7.2	Cisco AnyConnect Secure Mobility Client before 4.2.05015 and 4.3.x before 4.3.02039 mishandles pathnames, which allows local users	http://tools.cisco.com/security/center/content/CiscoSecurityA	A-CIS-ANYCO-210916/48

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

			to gain privileges via a crafted INF file, aka Bug ID CSCuz92464. **Reference: CVE-2016-6369**	dvisory/cisco-sa-20160824-anyconnect	
Application Policy Infrastructure Controller Enterprise Module *APIC-EM provides centralized automation of policy-based application profiles. Through programmability, automated network control helps IT rapidly respond to new business opportunities.*					
Execute Code	2016-08-18	8.5	The Grapevine update process in Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) 1.0 allows remote authenticated users to execute arbitrary commands as root via a crafted upgrade parameter, aka Bug ID CSCux15507. **Reference: CVE-2016-1365**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-apic	A-CIS-APPLI-210916/49
Connected Streaming Analytics *Connected Streaming Analytics (CSA) is an analytics platform that delivers predictive, actionable insights from high-velocity streams of live data from multiple sources, enabling real-time governance and immediate actions.*					
Gain Information	2016-08-22	4	Cisco Connected Streaming Analytics 1.1.1 allows remote authenticated users to discover a notification service password by reading administrative pages, aka Bug ID CSCuz92891. **Reference: CVE-2016-1477**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160810-csa	A-CIS-CONNE-210916/50
Firepower Management Center *Firepower Management Center provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. Firepower Management Center provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering,*					

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

and advanced malware protection.					
	2016-08-18	9	The web-based GUI in Cisco Firepower Management Center 4.x and 5.x before 5.3.0.3, 5.3.1.x before 5.3.1.2, and 5.4.x before 5.4.0.1 and Cisco Adaptive Security Appliance (ASA) Software on 5500-X devices with FirePOWER Services 4.x and 5.x before 5.3.0.3, 5.3.1.x before 5.3.1.2, and 5.4.x before 5.4.0.1 allows remote authenticated users to increase user-account privileges via crafted HTTP requests, aka Bug ID CSCur25483. **Reference: CVE-2016-1458**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-firepower	A-CIS-FIREP-210916/51
Execute Code	2016-08-18	9	The web-based GUI in Cisco Firepower Management Center 4.x and 5.x before 5.3.1.2 and 5.4.x before 5.4.0.1 and Cisco Adaptive Security Appliance (ASA) Software on 5500-X devices with FirePOWER Services 4.x and 5.x before 5.3.1.2 and 5.4.x before 5.4.0.1 allows remote authenticated users to execute arbitrary commands as root via crafted HTTP requests, aka Bug ID CSCur25513. **Reference: CVE-2016-1457**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-fmc	A-CIS-FIREP-210916/52

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

Cross-site scripting	2016-08-22	4.3	Cross-site scripting (XSS) vulnerability in Cisco Firepower Management Center 4.10.3, 5.2.0, 5.3.0, 5.3.0.2, 5.3.1, and 5.4.0 allows remote attackers to inject arbitrary web script or HTML via unspecified parameters, aka Bug IDs CSCur25508 and CSCur25518. **Reference: CVE-2016-6365**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-firepowermc	A-CIS-FIREP-210916/53
Firesight System Software Cisco Firesight System Software centralizes, integrates, and simplifies management. Firesight System Software provides complete and unified management over firewalls, application control, and intrusion prevention, URL filtering, and advanced malware protection.					
Bypass	2016-09-12	5	Cisco Firepower Management Center before 6.1 and FireSIGHT System Software before 6.1, when certain malware blocking options are enabled, allow remote attackers to bypass malware detection via crafted fields in HTTP headers, aka Bug ID CSCuz44482. **Reference: CVE-2016-6396**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160907-fsss1	A-CIS-FIRES-210916/54
Cross-site scripting	2016-09-12	3.5	Cross-site scripting (XSS) vulnerability in the web-based management interface in Cisco Firepower Management Center before 6.1 and FireSIGHT System Software before 6.1 allows remote authenticated users to inject arbitrary web script or HTML via a	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160907-fsss	A-CIS-FIRES-210916/55

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

			crafted URL, aka Bug ID CSCuz58658. **Reference: CVE-2016-6395**		
	2016-09-12	5.8	Session fixation vulnerability in Cisco Firepower Management Center and Cisco FireSIGHT System Software through 6.1.0 allows remote attackers to hijack web sessions via a session identifier, aka Bug ID CSCuz80503. **Reference: CVE-2016-6394**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160907-fsmc	A-CIS-FIRES-210916/56
Hosted Collaboration Mediation Fulfillment *Through Cisco Hosted Collaboration Mediation, NOC operators use a single dashboard that aggregates alarms from underlying domain managers.*					
Directory Traversal	2016-09-12	5	Directory traversal vulnerability in the web interface in Cisco Hosted Collaboration Mediation Fulfillment (HCM-F) 10.6(3) and earlier allows remote attackers to write to arbitrary files via a crafted URL, aka Bug ID CSCuz64717. **Reference: CVE-2016-6371**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-hcmf	A-CIS-HOSTE-210916/57
Directory Traversal	2016-09-12	4	Directory traversal vulnerability in the web interface in Cisco Hosted Collaboration Mediation Fulfillment (HCM-F) 10.6(3) and earlier allows remote authenticated users to read arbitrary files via a crafted pathname in an HTTP request, aka Bug ID CSCuz27255. **Reference: CVE-2016-**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-hcm	A-CIS-HOSTE-210916/58

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

			6370		
Identity Services Engine Software *Cisco Identity Services Engine (ISE) is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to the company’s routers and switches.*					
Cross-site scripting	2016-08-22	4.3	Cross-site scripting (XSS) vulnerability in Cisco Identity Services Engine 1.3(0.876) allows remote attackers to inject arbitrary web script or HTML via crafted parameters, aka Bug ID CSCva46497. **Reference: CVE-2016-1485**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ise	A-CIS-IDENT-210916/59
Media Origination System Suite *The Cisco Media Origination System (MOS) provides critical functions required to capture, store and originate media for multi-screen consumption.*					
Bypass	2016-09-03	6.8	Media Origination System Suite Software 2.6 and earlier in Cisco Virtual Media Packager (VMP) allows remote attackers to bypass authentication and make arbitrary Platform and Applications Manager (PAM) API calls via unspecified vectors, aka Bug ID CSCuz52110. **Reference: CVE-2016-6377**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-vmp	A-CIS-MEDIA-210916/60
Small Business 220 Series Smart Plus Switches *Cisco Small Business 220 Series Smart Plus Switches bridge the gap between managed and smart switches to offer customers the best of both worlds.*					
Gain Information	2016-09-01	10	Cisco Small Business 220 devices with firmware before 1.0.1.1 have a hardcoded SNMP community, which allows remote attackers to read or modify SNMP objects by leveraging knowledge of this community, aka	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-	A-CIS-SMALL-210916/61

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

			Bug ID CSCuz76216. **Reference: CVE-2016-1473**	sps3	
Small Business 220 Series Smart Plus Switches *Cisco Small Business 220 Series Smart Plus Switches bridge the gap between managed and smart switches to offer customers the best of both worlds.*					
Denial of Service	2016-09-01	5	The web-based management interface on Cisco Small Business 220 devices with firmware before 1.0.1.1 allows remote attackers to cause a denial of service (interface outage) via a crafted HTTP request, aka Bug ID CSCuz76238. **Reference: CVE-2016-1472**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps2	A-CIS-SMALL-210916/62
Cross-site scripting	2016-09-01	4.3	Cross-site scripting (XSS) vulnerability in the web-based management interface on Cisco Small Business 220 devices with firmware before 1.0.1.1 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCuz76232. **Reference: CVE-2016-1471**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps1	A-CIS-SMALL-210916/63
Cross Site Request Forgery	2016-09-01	6.8	Cross-site request forgery (CSRF) vulnerability in the web-based management interface on Cisco Small Business 220 devices with firmware before 1.0.1.1 allows remote attackers to hijack the authentication of arbitrary users, aka Bug ID CSCuz76230. **Reference: CVE-2016-1470**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-sps	A-CIS-SMALL-210916/64

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

Transport Gateway Installation Software *Transport Gateway Installation Software has access to the Call Home mailbox, in the event that the user wants to use the Transport Gateway to forward Call Home messages securely, using an SSL connection.*					
Cross-site scripting	2016-08-22	4.3	Cross-site scripting (XSS) vulnerability in Cisco Transport Gateway Installation Software 4.1(4.0) on Smart Call Home Transport Gateway devices allows remote attackers to inject arbitrary web script or HTML via a crafted value, aka Bug IDs CSCva40650 and CSCva40817. **Reference: CVE-2016-6359**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-sch	A-CIS-TRANS-210916/65
Unified Communications Manager *UCM brings together SSL VPN, security, application acceleration, and availability.*					
Bypass; Gain Information	2016-08-22	5	The User Data Services (UDS) API implementation in Cisco Unified Communications Manager 11.5 allows remote attackers to bypass intended access restrictions and obtain sensitive information via unspecified API calls, aka Bug ID CSCux67855. **Reference: CVE-2016-6364**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ucm	A-CIS-UNIFI-210916/66
Webex Meetings Server *WebEx combines desktop sharing through a web browser with phone conferencing and video, so everyone sees the same thing while you talk.*					
Bypass; Gain Information	2016-08-22	5	Cisco WebEx Meetings Server 2.6 allows remote attackers to bypass intended access restrictions and obtain sensitive application information via unspecified vectors, aka	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-WEBEX-210916/67

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

			Bug ID CSCuy92724. **Reference: CVE-2016-1484**	20160817-wms1	
Webex Wrf Player T29 *Through WebEx Player you can watch, share, and edit WebEx recordings.*					
Execute Code	2016-09-03	9.3	Cisco WebEx Meetings Player T29.10, when WRF file support is enabled, allows remote attackers to execute arbitrary code via a crafted file, aka Bug ID CSCva09375. **Reference: CVE-2016-1464**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-meetings-player	A-CIS-WEBEX-210916/68
Denial of Service	2016-09-03	4.3	Cisco WebEx Meetings Player T29.10, when WRF file support is enabled, allows remote attackers to cause a denial of service (application crash) via a crafted file, aka Bug ID CSCuz80455. **Reference: CVE-2016-1415**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-webex	A-CIS-WEBEX-210916/69
Wireless LAN Controller;Wireless LAN Controller 6.0;Wireless LAN Controller 7.0;Wireless LAN Controller 7.1;Wireless LAN Controller 7.2;Wireless LAN Controller 7.4 *Wireless LAN Controller optimizes the performance of your large wireless network with centralized control.*					

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

Denial of Service	2016-09-01	6.1	The Adaptive Wireless Intrusion Prevention System (wIPS) feature on Cisco Wireless LAN Controller (WLC) devices before 8.0.140.0, 8.1.x and 8.2.x before 8.2.121.0, and 8.3.x before 8.3.102.0 allows remote attackers to cause a denial of service (device restart) via a malformed wIPS packet, aka Bug ID CSCuz40263. **Reference: CVE-2016-6376**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-wlc-2	A-CIS-WIREL-210916/70
Citrix					
Xenapp; Xendesktop *Xenapp allows Windows applications to be accessed via individual devices from a shared server or cloud system; XenDesktop is a desktop virtualization software that allows multiple users to access and run Microsoft Windows desktops that are installed at a centralized location separate from the devices from which they are being accessed.*					
NA	2016-08-19	7.5	Citrix XenApp 6.x before 6.5 HRP07 and 7.x before 7.9 and Citrix XenDesktop before 7.9 might allow attackers to weaken an unspecified security mitigation via vectors related to memory permission. **Reference: CVE-2016-6493**	http://support.citrix.com/article/CTX215460	A-CIT-XENAP-210916/71
Clip-bucket *Clip-Bucket is committed to delivering an Unparalleled Entertainment Experience, and we do so by Engaging and Empowering our Content-Providers and Audience every step of the way - from Complete Multimedia Management of Videos, Photos & Audios to the Enhanced Social networking Features like Channels, Collections, Friends, Messages & Feeds.*					
Cross-site scripting	2016-09-01	4.3	Cross-site scripting (XSS) vulnerability in ClipBucket before 2.8.1 RC2 allows remote attackers to inject	https://github.com/arslancb/clipbucket/c	A-CLI-CLIPB-210916/72

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

			arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-4848**	ommit/ff5e37d3e1098a7ce2b9fe60389b14514932dd93	
Dotnetnuke *Dotnetnuke is the leading open source web content management platform (CMS) in the Microsoft ecosystem.*					
Cross-site scripting	2016-08-31	3.5	Cross-site scripting (XSS) vulnerability in the user-profile biography section in DotNetNuke (DNN) before 8.0.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted onclick attribute in an IMG element. **Reference: CVE-2016-7119**	http://www.dnnsoftware.com/community/security/security-center	A-DOT-DOTNE-210916/73
Drupal					
Drupal *Drupal is a scalable, open platform for web content management and digital experiences. Drupal provides deep capabilities and endless flexibility on the web.*					
Bypass; Gain Information	2016-09-09	5	The Views module 7.x-3.x before 7.x-3.14 in Drupal 7.x and the Views module in Drupal 8.x before 8.1.3 might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors. **Reference: CVE-2016-6212**	https://www.drupal.org/SA-CORE-2016-002	A-DRU-DRUPA-210916/74
EMC					
Authentication Manager Prime Self-service *RSA Authentication Manager: Platform behind RSA SecurID that allows for centralized management of the RSA SecurID environment including authentication methods, users, applications, and agents across multiple physical sites. It verifies authentication requests and centrally administers authentication policies for*					

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

organizations' end users.					
Denial of Service	2016-08-22	5.5	The Self-Service Portal in EMC RSA Authentication Manager (AM) Prime Self-Service 3.0 and 3.1 before 3.1 1915.42871 allows remote authenticated users to cause a denial of service (PIN change for an arbitrary user) via a modified token serial number within a PIN change request, related to a "direct object reference vulnerability." **Reference: CVE-2016-0915**	http://seclists.org/bugtraq/2016/Aug/71	A-EMC-AUTHE-210916/75
GNU					
Libidn *Libidn is developed for the GNU/Linux system, but runs on over 20 Unix platforms.*					
Denial of Service	2016-09-07	5	The stringprep_utf8_nfkc_normalize function in lib/nfkc.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via crafted UTF-8 data. **Reference: CVE-2016-6263**	http://git.savannah.gnu.org/cgit/libidn.git/commit/?id=1fbee57ef3c72db2206dd87e4162108b2f425555	A-GNU-LIBID-210916/76
Mailman *GNU Mailman is a computer software application from the GNU Project for managing electronic mailing lists.*					
Cross Site Request Forgery	2016-09-02	6.8	Cross-site request forgery (CSRF) vulnerability in the admin web interface in GNU Mailman before 2.1.15 allows remote attackers to hijack the authentication of administrators. **Reference: CVE-2016-**	https://bugs.launchpad.net/bugs/1614841	A-GNU-MAILM-210916/77

			7123		
Cross Site Request Forgery	2016-09-02	6.8	Cross-site request forgery (CSRF) vulnerability in the user options page in GNU Mailman 2.1.x before 2.1.23 allows remote attackers to hijack the authentication of arbitrary users for requests that modify an option, as demonstrated by gaining access to the credentials of a victim's account. **Reference: CVE-2016-6893**	https://bugs.launchpad.net/bugs/1614841	A-GNU-MAILM-210916/78
Google					
Chrome *Google Chrome is a freeware web browser developed by Google.*					
Denial of Service	2016-09-11	6.8	SkPath.cpp in Skia, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, does not properly validate the return values of ChopMonoAtY calls, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via crafted graphics data. **Reference: CVE-2016-7395**	https://codereview.chromium.org/2006143009	A-GOO-CHROM-210916/79
Denial of Service	2016-09-11	7.5	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.89 on Windows and OS X and	https://googlechromereleases.blogspot.com/2016/08/st	A-GOO-CHROM-210916/80

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

			before 53.0.2785.92 on Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors. **Reference: CVE-2016-5167**	able-channel-update-for-desktop_31.html	
Gain Information	2016-09-11	2.6	The download implementation in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly restrict saving a file:// URL that is referenced by an http:// URL, which makes it easier for user-assisted remote attackers to discover NetNTLM hashes and conduct SMB relay attacks via a crafted web page that is accessed with the "Save page as" menu choice. **Reference: CVE-2016-5166**	https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	A-GOO-CHROM-210916/81
Cross-site scripting	2016-09-11	4.3	Cross-site scripting (XSS) vulnerability in the Developer Tools (aka DevTools) subsystem in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux allows remote attackers to inject arbitrary web script or HTML via the settings parameter in a chrome-devtools-frontend.appspot.com	https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	A-GOO-CHROM-210916/82

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

			URL's query string. **Reference: CVE-2016-5165**		
Cross-site scripting	2016-09-11	4.3	Cross-site scripting (XSS) vulnerability in WebKit/Source/platform/v8_inspector/V8Debugger.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to inject arbitrary web script or HTML into the Developer Tools (aka DevTools) subsystem via a crafted web site, aka "Universal XSS (UXSS)." **Reference: CVE-2016-5164**	https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	A-GOO-CHROM-210916/83
	2016-09-11	4.3	The bidirectional-text implementation in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not ensure left-to-right (LTR) rendering of URLs, which allows remote attackers to spoof the address bar via crafted right-to-left (RTL) Unicode text, related to omnibox/SuggestionView.java and omnibox/UrlBar.java in Chrome for Android. **Reference: CVE-2016-5163**	https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	A-GOO-CHROM-210916/84
NA	2016-09-11	4.3	The AllowCrossRendererReso	https://googlechromer	A-GOO-CHROM-

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

			urceLoad function in extensions/browser/url_request_util.cc in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly use an extension's manifest.json web_accessible_resources field for restrictions on IFRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks, and trick users into changing extension settings, via a crafted web site, a different vulnerability than CVE-2016-5160. **Reference: CVE-2016-5162**	eleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	210916/85
Denial of Service	2016-09-11	6.8	The EditingStyle::mergeStyle function in WebKit/Source/core/editing/EditingStyle.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, mishandles custom properties, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site that leverages "type confusion" in the StylePropertySerializer class.	https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	A-GOO-CHROM-210916/86

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

			Reference: CVE-2016-5161		
NA	2016-09-11	4.3	The AllowCrossRendererResourceLoad function in extensions/browser/url_request_util.cc in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly use an extension's manifest.json web_accessible_resources field for restrictions on IFRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks, and trick users into changing extension settings, via a crafted web site, a different vulnerability than CVE-2016-5162. **Reference: CVE-2016-5160**	https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	A-GOO-CHROM-210916/87
Denial of Service; Memory Overflow	2016-09-11	6.8	Multiple integer overflows in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data that is mishandled during opj_aligned_malloc calls	https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	A-GOO-CHROM-210916/88

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

			in dwt.c and t1.c. **Reference: CVE-2016-5159**		
Denial of Service Overflow	2016-09-11	6.8	Multiple integer overflows in the opj_tcd_init_tile function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data. **Reference: CVE-2016-5158**	https://crbug.com/628890	A-GOO-CHROM-210916/89
Execute Code; Overflow	2016-09-11	6.8	Heap-based buffer overflow in the opj_dwt_interleave_v function in dwt.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to execute arbitrary code via crafted coordinate values in JPEG 2000 data. **Reference: CVE-2016-5157**	https://pdfium.googlesource.com/pdfium/+/b6befb2ed2485a3805cddea86dc7574510178ea9	A-GOO-CHROM-210916/90
Denial of Service	2016-09-11	6.8	extensions/renderer/event_bindings.cc in the event bindings in Google Chrome before 53.0.2785.89 on Windows and OS X and	https://googlechromereleases.blogspot.com/2016/08/stable-	A-GOO-CHROM-210916/91

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

			before 53.0.2785.92 on Linux attempts to process filtered events after failure to add an event matcher, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors. **Reference: CVE-2016-5156**	channel-update-for-desktop_31.html	
	2016-09-11	4.3	Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly validate access to the initial document, which allows remote attackers to spoof the address bar via a crafted web site. **Reference: CVE-2016-5155**	https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	A-GOO-CHROM-210916/92
Denial of Service Overflow	2016-09-11	6.8	Multiple heap-based buffer overflows in PDFium, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted JBig2 image. **Reference: CVE-2016-5154**	https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	A-GOO-CHROM-210916/93
Denial of Service	2016-09-11	6.8	The Web Animations implementation in Blink, as used in Google Chrome before	https://googlechromereleases.blogspot.com/	A-GOO-CHROM-210916/94

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

			53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, improperly relies on list iteration, which allows remote attackers to cause a denial of service (use-after-destruction) or possibly have unspecified other impact via a crafted web site. **Reference: CVE-2016-5153**	2016/08/stable-channel-update-for-desktop_31.html	
Denial of Service Overflow	2016-09-11	6.8	Integer overflow in the opj_tcd_get_decoded_tile_size function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data. **Reference: CVE-2016-5152**	https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html	A-GOO-CHROM-210916/95
Denial of Service	2016-09-11	6.8	PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux mishandles timers, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted PDF	https://crbug.com/634716	A-GOO-CHROM-210916/96

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

			document, related to fpdfsdk/javascript/JS_Object.cpp and fpdfsdk/javascript/app.cpp. **Reference: CVE-2016-5151**		
Denial of Service	2016-09-11	6.8	WebKit/Source/bindings/modules/v8/V8BindingForModules.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, has an Indexed Database (aka IndexedDB) API implementation that does not properly restrict key-path evaluation, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code that leverages certain side effects. **Reference: CVE-2016-5150**	https://codereview.chromium.org/2255413004/	A-GOO-CHROM-210916/97
NA	2016-09-11	6.8	The extensions subsystem in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux relies on an IFRAME source URL to identify an associated extension, which allows remote attackers to conduct extension-bindings injection attacks by	https://codereview.chromium.org/2208483002/	A-GOO-CHROM-210916/98

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

			leveraging script access to a resource that initially has the about:blank URL. **Reference: CVE-2016-5149**		
Cross-site scripting	2016-09-11	4.3	Cross-site scripting (XSS) vulnerability in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to inject arbitrary web script or HTML via vectors related to widget updates, aka "Universal XSS (UXSS)." **Reference: CVE-2016-5148**	https://codereview.chromium.org/2134113002	A-GOO-CHROM-210916/99
Cross-site scripting	2016-09-11	4.3	Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, mishandles deferred page loads, which allows remote attackers to inject arbitrary web script or HTML via a crafted web site, aka "Universal XSS (UXSS)." **Reference: CVE-2016-5147**	https://codereview.chromium.org/2155393002	A-GOO-CHROM-210916/100
Gree					
Jose-php *jose-php makes it easier for remote attackers to obtain sensitive information via a timing attack, related to JWE.php and JWS.php*					

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

NA	2016-09-03	5	The RSA 1.5 algorithm implementation in the JOSE_JWE class in JWE.php in jose-php before 2.2.1 lacks the Random Filling protection mechanism, which makes it easier for remote attackers to obtain cleartext data via a Million Message Attack (MMA). **Reference: CVE-2016-5430**	https://github.com/nov/jose-php/commit/f03b986b4439e20b0fd635109b48afe96cf0099b#diff-37b0d289d6375ba4a7740401950ccdd6R199	A-GRE-JOSE--210916/101
Gain Information	2016-09-03	4.3	jose-php before 2.2.1 does not use constant-time operations for HMAC comparison, which makes it easier for remote attackers to obtain sensitive information via a timing attack, related to JWE.php and JWS.php. **Reference: CVE-2016-5429**	https://github.com/nov/jose-php/commit/f03b986b4439e20b0fd635109b48afe96cf0099b#diff-37b0d289d6375ba4a7740401950ccdd6R287	A-GRE-JOSE--210916/102
HP					
Converged Infrastructure Solution Sizer Suite; Insight Management Sizer; Power Advisor; Sap Sizing Tool; Sizer For Converged Systems Virtualization; Sizer For Microsoft Exchange Server 2010;Sizer For Microsoft Exchange Server 2013;Sizer For Microsoft Exchange Server 2016;Sizer For Microsoft Lync Server 2013;Sizer For Microsoft Sharepoint 2010;Sizer For Microsoft Sharepoint 2013;Sizer For Microsoft Skype For Business Server 2015;Sizing Tool For Sap Business Suite Powered By Hana; Storage Sizing Tool; Synergy Planning Tool *Hewlett Packard Enterprise Solution Sizers are automated tools that assist with recommending a solution environment; HP Power Advisor is an easy-to-use tool that estimates your data center power requirements for your server and storage configurations; Sizing is the process of determining the hardware requirements to implement SAP. HP has developed the HP Sizer for Microsoft exchange to assist customers with proper server and storage sizing and configuration for their*					

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

Exchange deployments; Hewlett Packard Enterprise Solution Sizers are automated tools that assist with recommending a solution environment; The HPE Sizing Tool for SAP Business Suite powered by HANA provides end users with a simple and reliable way to choose their project hardware; HPE Synergy Planning Tool provides meaningful information for build outs and installation verifications, and power and weight needs for HPE Synergy solutions.					
Execute Code	2016-08-22	7.6	HPE Smart Update in Storage Sizing Tool before 13.0, Converged Infrastructure Solution Sizer Suite (CISSS) before 2.13.1, Power Advisor before 7.8.2, Insight Management Sizer before 16.12.1, Synergy Planning Tool before 3.3, SAP Sizing Tool before 16.12.1, Sizing Tool for SAP Business Suite powered by HANA before 16.11.1, Sizer for ConvergedSystems Virtualization before 16.7.1, Sizer for Microsoft Exchange Server before 16.12.1, Sizer for Microsoft Lync Server 2013 before 16.12.1, Sizer for Microsoft SharePoint 2013 before 16.13.1, Sizer for Microsoft SharePoint 2010 before 16.11.1, and Sizer for Microsoft Skype for Business Server 2015 before 16.5.1 allows remote attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-4377**	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05237578	A-HP-CONVE-210916/103
Operations Manager *HP Operations Manager is a System monitoring package manufactured by Hewlett-Packard (HP).*					
Cross-site scripting	2016-09-08	3.5	Cross-site scripting (XSS) vulnerability in the AdminUI in HPE Operations Manager	https://h20566.www2.hpe.com/portal/site	A-HP-OPERA-210916/104

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

			9.21.x before 9.21.130 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-4380**	/hpsc/public/kb/docDisplay?docId=emr_na-c05249833	
Xp 9000 Command View;Xp7 Command View *HP XP P9000 Command View Advanced Edition Software is a full-featured device manager for the HP XP P9500 and XP Disk Array products.*					
Gain Information	2016-08-26	5	The (1) Device Manager, (2) Tiered Storage Manager, (3) Replication Manager, (4) Replication Monitor, and (5) Hitachi Automation Director (HAD) components in HPE XP P9000 Command View Advanced Edition Software before 8.4.1-00 and XP7 Command View Advanced Edition Suite before 8.4.1-00 allow remote attackers to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-4378**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05241355	A-HP-XP 90-210916/105
Bypass	2016-09-08	4.4	HPE XP7 Command View Advanced Edition (CVAE) Suite 6.x through 8.x before 8.4.1-02, when Replication Manager (RepMgr) and Device Manager (DevMgr) are enabled, allows local users to bypass intended access restrictions via unspecified vectors. **Reference: CVE-2016-4381**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05257711	A-HP-XP7 C-210916/106
Huawei					

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

E9000 Chassis *The Huawei E9000 server converged-architecture blade server enables convergence of computing, storage, networking, and management.*					
Denial of Service	2016-09-07	4.9	XML external entity (XXE) vulnerability in the Hyper Management Module (HMM) in Huawei E9000 rack servers with software before V100R001C00SPC296 allows remote authenticated users to read arbitrary files or cause a denial of service (web service outage) via a crafted XML document. **Reference: CVE-2016-6898**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160824-01-e9000-en	A-HUA-E9000-210916/107
Fusionaccess *FusionCloud Desktop virtualizes and centralizes PC computing and storage resources in the data center, creating a Virtual Desktop Infrastructure (VDI).*					
Http R.Spl.	2016-09-07	4.3	CRLF injection vulnerability in Huawei FusionAccess before V100R006C00 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors. **Reference: CVE-2016-6839**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160817-01-fusionaccess-en	A-HUA-FUSIO-210916/108
UMA *Huawei's Unified Maintenance Audit (UMA) system centrally manages, monitors, and audits operations of all Operation and Maintenance (O&M) personnel in an enterprise.*					
Execute Code	2016-09-07	10	Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 allows remote attackers to execute arbitrary commands via "special characters," a different	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160824-01-uma-	A-HUA-UMA-210916/109

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

			vulnerability than CVE-2016-7109. **Reference: CVE-2016-7110**	en	
Execute Code	2016-09-07	10	Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 allows remote attackers to execute arbitrary commands via "special characters," a different vulnerability than CVE-2016-7110. **Reference: CVE-2016-7109**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160824-01-uma-en	A-HUA-UMA-210916/110
Gain Information	2016-09-07	4	Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 SPH206 allows remote authenticated users to obtain the MD5 hashes of arbitrary user passwords via unspecified vectors. **Reference: CVE-2016-7108**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160824-02-uma-en	A-HUA-UMA-210916/111
NA	2016-09-07	5	Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 SPH206 allows remote attackers to reset arbitrary user passwords and consequently affect system data integrity via unspecified vectors. **Reference: CVE-2016-7107**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160824-02-uma-en	A-HUA-UMA-210916/112
IBM					
Bigfix Platform *The IBM BigFix platform is a multi-layered technology platform that acts as the core part of the global IT infrastructure.*					

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

Cross-site scripting	2016-08-31	4.3	Cross-site scripting (XSS) vulnerability in IBM BigFix Platform (formerly Tivoli Endpoint Manager) 9.x before 9.1.8 and 9.2.x before 9.2.8 allows remote attackers to inject arbitrary web script or HTML via a modified .beswrpt file. **Reference: CVE-2016-0293**	http://www-01.ibm.com/support/docview.wss?uid=swg21985743	A-IBM-BIGFI-210916/113
Gain Information	2016-08-30	4.3	WebReports in IBM BigFix Platform (formerly Tivoli Endpoint Manager) 9.x before 9.5.2 allows remote attackers to obtain sensitive information by sniffing the network for HTTP traffic. **Reference: CVE-2016-0397**	http://www-01.ibm.com/support/docview.wss?uid=swg21985907	A-IBM-BIGFI-210916/114
Gain Information	2016-08-30	2.1	WebReports in IBM BigFix Platform (formerly Tivoli Endpoint Manager) 9.x before 9.5.2 allows local users to discover the cleartext system password by reading a report. **Reference: CVE-2016-0292**	http://www-01.ibm.com/support/docview.wss?uid=swg21985907	A-IBM-BIGFI-210916/115
Connections *'Connections' allows your organization to engage the right people, accelerate innovation and deliver results.*					
Cross-site scripting	2016-09-01	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 4.0 through CR4, 4.5 through CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via	http://www-01.ibm.com/support/docview.wss?uid=swg21988991	A-IBM-CONNE-210916/116

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

			unspecified vectors, a different vulnerability than CVE-2016-2995, CVE-2016-2997, and CVE-2016-3005. **Reference: CVE-2016-3010**		
Cross-site scripting	2016-09-01	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 5.0 before CR4 and 5.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-2954 and CVE-2016-2956. **Reference: CVE-2016-3008**	http://www-01.ibm.com/support/docview.wss?uid=swg21988990	A-IBM-CONNE-210916/117
Cross-site scripting	2016-09-01	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 4.0 through CR4, 4.5 through CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-2995, CVE-2016-2997, and CVE-2016-3010. **Reference: CVE-2016-3005**	http://www-01.ibm.com/support/docview.wss?uid=swg21988991	A-IBM-CONNE-210916/118
Cross Site Request Forgery	2016-09-01	3.5	Cross-site request forgery (CSRF) vulnerability in IBM Connections 4.0 through CR4, 4.5 through CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated	http://www-01.ibm.com/support/docview.wss?uid=swg2	A-IBM-CONNE-210916/119

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

			users to hijack the authentication of arbitrary users for requests that update data. **Reference: CVE-2016-2998**	1988991	
Cross-site scripting	2016-09-01	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 4.0 through CR4, 4.5 through CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-2995, CVE-2016-3005, and CVE-2016-3010. **Reference: CVE-2016-2997**	http://www-01.ibm.com/support/docview.wss?uid=swg21988991	A-IBM-CONNE-210916/120
Cross-site scripting	2016-09-01	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 4.0 through CR4, 4.5 through CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-2997, CVE-2016-3005, and CVE-2016-3010. **Reference: CVE-2016-2995**	http://www-01.ibm.com/support/docview.wss?uid=swg21988991	A-IBM-CONNE-210916/121
Cross-site scripting	2016-09-01	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 5.0 before CR4 and 5.5 before CR1 allows remote authenticated users to	http://www-01.ibm.com/support/docview.wss?	A-IBM-CONNE-210916/122

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

			inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-2954 and CVE-2016-3008. **Reference: CVE-2016-2956**	uid=swg21988990	
Cross-site scripting	2016-09-01	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 5.0 before CR4 and 5.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2016-2956 and CVE-2016-3008. **Reference: CVE-2016-2954**	http://www-01.ibm.com/support/docview.wss?uid=swg21988990	A-IBM-CONNE-210916/123
Cross-site scripting	2016-08-31	3.5	Cross-site scripting (XSS) vulnerability in IBM Forms Experience Builder 8.5.x and 8.6.x before 8.6.3 allows remote authenticated users to inject arbitrary web script or HTML via crafted input to an application that was built with this product. **Reference: CVE-2016-0370**	http://www-01.ibm.com/support/docview.wss?uid=swg21988726	A-IBM-FORMS-210916/124
Rational Collaborative Lifecycle Management; Rational Team Concert *IBM Rational Collaborative Lifecycle Management is an application lifecycle management solution that includes IBM Rational Team Concert.*					
Cross-site scripting	2016-09-12	3.5	Cross-site scripting (XSS) vulnerability in IBM Rational Team Concert 6.0.1 and 6.0.2 before 6.0.2 iFix2 and Rational Collaborative Lifecycle Management 6.0.1 and	http://www-01.ibm.com/support/docview.wss?uid=swg2	A-IBM-RATIO-210916/125

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

			6.0.2 before 6.0.2 iFix2 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-0331**	1989899	
Tivoli Storage Manager For Space Management *Tivoli Storage Manager for Space Management to move inactive or seldom-used files to server storage, freeing disk space for active data.*					
Gain Information	2016-09-12	2.1	IBM Tivoli Storage Manager for Space Management (aka Spectrum Protect for Space Management) 6.3.x before 6.3.2.6, 6.4.x before 6.4.3.3, and 7.1.x before 7.1.6, when certain dsmsetpw tracing is configured, allows local users to discover an encrypted password by reading application-trace output. **Reference: CVE-2016-5927**	http://www-01.ibm.com/support/docview.wss?uid=swg21989006	A-IBM-TIVOL-210916/126
Websphere Application Server *IBM WebSphere Application Server is the leading open standards-based application foundation offering accelerated delivery of innovative applications and unmatched operational efficiency, reliability, administration, security, and control.*					
Overflow; Gain Info	2016-09-01	3.5	Buffer overflow in IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.43, 8.0 before 8.0.0.13, 8.5 before 8.5.5.10, 9.0 before 9.0.0.1, and Liberty before 16.0.0.3, when HttpSessionIdReuse is enabled, allows remote authenticated users to obtain sensitive information via	http://www-01.ibm.com/support/docview.wss?uid=swg21982588	A-IBM-WEBSP-210916/127

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

			unspecified vectors. **Reference: CVE-2016-0385**		
Websphere Portal *IBM WebSphere Portal is a set of software tools that enables companies to build and manage web portals.*					
Denial of Service	2016-09-12	4	IBM WebSphere Portal 6.1.0 through 6.1.0.6 CF27, 6.1.5 through 6.1.5.3 CF27, 7.0.0 through 7.0.0.2 CF30, 8.0.0 through 8.0.0.1 CF21, and 8.5.0 before CF12 allows remote authenticated users to cause a denial of service by uploading temporary files. **Reference: CVE-2016-5954**	http://www-01.ibm.com/support/docview.wss?uid=swg21989993	A-IBM-WEBSP-210916/128
Jwcrypto Project					
Jwcrypto *JWCrypto is an implementation of the Javascript Object Signing and Encryption (JOSE) Web Standards as they are being developed in the JOSE IETF Working Group and related technology.*					
Gain Information	2016-09-01	4.3	The _Rsa15 class in the RSA 1.5 algorithm implementation in jwa.py in jwcrypto before 0.3.2 lacks the Random Filling protection mechanism, which makes it easier for remote attackers to obtain cleartext data via a Million Message Attack (MMA). **Reference: CVE-2016-6298**	https://github.com/latchset/jwcrypto/releases/tag/v0.3.2	A-JWC-JWCRY-210916/129
Kaspersky					

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

Safe Browser *Kaspersky Safe Browser by filtering out malicious links and inappropriate content and helping you to avoid phishing websites that may try to steal your confidential information and your identity Kaspersky Safe Browser helps you safely surf the Web on your iPhone, iPad or Windows Phone device.*					
Gain Information	2016-08-25	4.3	Kaspersky Safe Browser iOS before 1.7.0 does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to obtain sensitive information via a crafted certificate. **Reference: CVE-2016-6231**	https://support.kaspersky.com/vulnerability.aspx?el=12430#280716	A-KAS-SAFE-210916/130
Let's Php!					
Simple Chat *This class implements a simple Web and MySQL based chat system.It generates HTML and JavaScript to display a chat box and a form input to submit new chat line entries using AJAX to avoid page reloading.*					
Cross-site scripting	2016-09-01	4.3	Cross-site scripting (XSS) vulnerability in Let's PHP! simple chat before 2016-08-15 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-4851**	NA	A-LET-SIMPL-210916/131
Mac-telnet					
Mac-telnet *Open source MAC Telnet client and server for connecting to Mikrotik RouterOS routers and Linux machines via MAC address.*					
Execute Code; Overflow	2016-08-30	7.5	Buffer overflow in the handle_packet function in mactelnet.c in the client in MAC-Telnet 0.4.3 and earlier allows remote TELNET servers to execute arbitrary code via a long string in an MT_CPTYPE_PASSSALT control packet.	https://github.com/haakonnessjoen/MAC-Telnet/pull/20	A-MAC-MAC-T-210916/132

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

			Reference: CVE-2016-7115		
Microsoft					
Edge *Microsoft Edge is a web browser developed by Microsoft and included in the company's Windows 10 operating systems, replacing Internet Explorer as the default web browser on all device classes.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	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-2016-3350. **Reference: CVE-2016-3377**	http://technet.microsoft.com/en-us/security/bulletin/ms16-105	A-MIC-EDGE-210916/133
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	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-2016-3377. **Reference: CVE-2016-3350**	http://technet.microsoft.com/en-us/security/bulletin/ms16-105	A-MIC-EDGE-210916/134
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability,"	http://technet.microsoft.com/en-us/security/bulletin/ms16-105	A-MIC-EDGE-210916/135

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

			a different vulnerability than CVE-2016-3294. **Reference: CVE-2016-3330**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3330. **Reference: CVE-2016-3294**	http://technet.microsoft.com/en-us/security/bulletin/ms16-105	A-MIC-EDGE-210916/136

Edge; Internet Explorer

Microsoft Edge is a web browser developed by Microsoft and included in the company's Windows 10 operating systems, replacing Internet Explorer as the default web browser on all device classes; Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems, starting in 1995.

Gain Information	2016-09-14	2.6	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability." **Reference: CVE-2016-3351**	NA	A-MIC-EDGE-210916/137
Gain Information	2016-09-14	2.6	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability." **Reference: CVE-2016-3325**	NA	A-MIC-EDGE-210916/138

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

Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	6.8	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." **Reference: CVE-2016-3297**	NA	A-MIC-EDGE-210916/139
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	5.1	Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." **Reference: CVE-2016-3295**	NA	A-MIC-EDGE-210916/140
Gain Information	2016-09-14	2.6	Microsoft Internet Explorer 11 and Microsoft Edge mishandle cross-origin requests, which allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability." **Reference: CVE-2016-3291**	NA	A-MIC-EDGE-210916/141
Denial of Service; Execute Code; Overflow; Memory	2016-09-14	5.1	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory	NA	A-MIC-EDGE-210916/142

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

Corruption			corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." **Reference: CVE-2016-3247**		
Excel *Microsoft Excel is a spreadsheet developed by Microsoft for Windows, Mac OS X, Android and iOS.*					
Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	Microsoft Excel 2010 SP2 allows remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3361**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-EXCEL-210916/143
Excel; Excel For Mac; Excel Viewer; Office Compatibility Pack; Office Online Server; Sharepoint Designer *In Compatibility Pack (in addition to Microsoft Office 2000, Office XP, or Office 2003), you will be able to open, edit, and save files using the file formats in newer versions of Word, Excel, and PowerPoint*					
Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel 2016 for Mac, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Automation Services on SharePoint Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-EXCEL-210916/144

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

			3358		
Excel; Excel Viewer; Office Compatibility Pack *Excel Viewer contains data in tabular forms. It is one of the important document file format; In Compatibility Pack (in addition to Microsoft Office 2000, Office XP, or Office 2003), you will be able to open, edit, and save files using the file formats in newer versions of Word, Excel, and PowerPoint*					
Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3363. **Reference: CVE-2016-3381**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-EXCEL-210916/145
Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3381. **Reference: CVE-2016-3363**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-EXCEL-210916/146
Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-EXCEL-210916/147

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

			"Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3359**		
Excel; Excel Viewer; Office Compatibility Pack; Office Online Server; Sharepoint Designer *Excel Viewer contains data in tabular forms. It is one of the important document file format; In Compatibility Pack (in addition to Microsoft Office 2000, Office XP, or Office 2003), you will be able to open, edit, and save files using the file formats in newer versions of Word, Excel, and PowerPoint; SharePoint Designer is the tool of choice for the rapid development of SharePoint applications.*					
Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Automation Services on SharePoint Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3362. **Reference: CVE-2016-3365**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-EXCEL-210916/148
Excel; Excel Viewer; Office Compatibility Pack; Office Online Server; Sharepoint Designer *Compatibility Pack in addition to Microsoft Office 2000, Office XP, or Office 2003, you will be able to open, edit, and save files using the file formats in newer versions of Word, Excel, and PowerPoint .SharePoint Designer is the tool of choice for the rapid development of SharePoint applications.*					

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

Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Automation Services on SharePoint Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3365. **Reference: CVE-2016-3362**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-EXCEL-210916/149
Exchange Server *Microsoft Exchange Server is a mail server and calendaring server developed by Microsoft.*					
Cross-site scripting	2016-09-14	4.3	Cross-site scripting (XSS) vulnerability in Microsoft Exchange Server 2016 Cumulative Update 1 and 2 allows remote attackers to inject arbitrary web script or HTML via a meeting-invitation request, aka "Microsoft Exchange Elevation of Privilege Vulnerability." **Reference: CVE-2016-3379**	http://technet.microsoft.com/en-us/security/bulletin/ms16-108	A-MIC-EXCHA-210916/150
NA	2016-09-14	5.8	Open redirect vulnerability in Microsoft Exchange Server 2013 SP1, 2013 Cumulative Update 12, 2013	http://technet.microsoft.com/en-us/securit	A-MIC-EXCHA-210916/151

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

			Cumulative Update 13, 2016 Cumulative Update 1, and 2016 Cumulative Update 2 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a crafted URL, aka "Microsoft Exchange Open Redirect Vulnerability." **Reference: CVE-2016-3378**	y/bulletin/ms16-108	
Gain Information	2016-09-14	4	Microsoft Exchange Server 2007 SP3, 2010 SP3, 2013 SP1, 2013 Cumulative Update 12, 2013 Cumulative Update 13, 2016 Cumulative Update 1, and 2016 Cumulative Update 2 misparses e-mail messages, which allows remote authenticated users to obtain sensitive Outlook application information by leveraging the Send As right, aka "Microsoft Exchange Information Disclosure Vulnerability." **Reference: CVE-2016-0138**	http://technet.microsoft.com/en-us/security/bulletin/ms16-108	A-MIC-EXCHA-210916/152
Internet Explorer *Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems, starting in 1995.*					
Bypass	2016-09-14	5.1	Microsoft Internet Explorer 9 through 11 mishandles .url files from the Internet zone, which allows remote attackers to bypass intended access restrictions via a crafted file, aka "Internet Explorer	http://technet.microsoft.com/en-us/security/bulletin/ms16-104	A-MIC-INTER-210916/153

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

			Security Feature Bypass." **Reference: CVE-2016-3353**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	6.8	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability." **CVE-2016-3324**	http://technet.microsoft.com/en-us/security/bulletin/ms16-104	A-MIC-INTER-210916/154
Bypass	2016-09-14	5.1	Microsoft Internet Explorer 10 and 11 mishandles integrity settings and zone settings, which allows remote attackers to bypass a sandbox protection mechanism via a crafted web site, aka "Internet Explorer Elevation of Privilege Vulnerability." **Reference: CVE-2016-3292**	http://technet.microsoft.com/en-us/security/bulletin/ms16-104	A-MIC-INTER-210916/155
Office *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft.*					
Gain Information	2016-09-14	4.3	The Visual Basic macros in Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, and 2016 export a certificate-store private key during a document-save operation, which allows attackers to obtain sensitive information via unspecified vectors, aka "Microsoft Information Disclosure Vulnerability." **Reference: CVE-2016-**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-OFFIC-210916/156

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

			0141		
Bypass	2016-09-14	4.3	The Click-to-Run (C2R) implementation in Microsoft Office 2013 SP1 and 2016 allows local users to bypass the ASLR protection mechanism via a crafted application, aka "Microsoft APP-V ASLR Bypass." **Reference: CVE-2016-0137**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-OFFIC-210916/157
Office Compatibility Pack; Office Web Apps; Office Web Apps Server; Powerpoint; Powerpoint For Mac; Powerpoint Viewer; Sharepoint Designer *Compatibility Pack in addition to Microsoft Office 2000, Office XP, or Office 2003, you will be able to open, edit, and save files using the file formats in newer versions of Word, Excel, and PowerPoint; SharePoint Designer is the tool of choice for the rapid development of SharePoint applications.; Powerpoint is an MS Office tool.*					
Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	Microsoft PowerPoint 2007 SP3, PowerPoint 2010 SP2, PowerPoint 2013 SP1, PowerPoint 2013 RT SP1, PowerPoint 2016 for Mac, Office Compatibility Pack SP3, PowerPoint Viewer, SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3360**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-OFFIC-210916/158
Office; Office Web Apps; Office Web Apps Server; Sharepoint Foundation; Word For Mac; Word Viewer *When used with SharePoint 2013 on-premises, Office Web Apps provides updated versions of Word Web App, Excel Web App, PowerPoint Web App, and OneNote Web App; SharePoint Designer is the tool of choice for the rapid development of SharePoint applications; Word for MAC and Word Viewer are MS Applications.*					

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

Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, Office 2016, Word for Mac 2011, Word 2016 for Mac, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, SharePoint Server 2013 SP1, Excel Automation Services on SharePoint Server 2013 SP1, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3357**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-OFFIC-210916/159
Outlook; Outlook 2013 Rt *Microsoft Outlook is a personal information manager from Microsoft, available as a part of the Microsoft Office suite.*					
Bypass	2016-09-14	4.3	Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, Outlook 2016, and Outlook 2016 for Mac do not properly implement RFC 2046, which allows remote attackers to bypass virus or spam detection via crafted MIME data in an e-mail attachment, aka "Microsoft Office Spoofing Vulnerability." **Reference: CVE-2016-**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-OUTLO-210916/160

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

			3366		
Silverlight *Microsoft Silverlight is an application framework for writing and running rich Internet applications.*					
Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	StringBuilder in Microsoft Silverlight 5 before 5.1.50709.0 does not properly allocate memory for string-insert and string-append operations, which allows remote attackers to execute arbitrary code via a crafted web site, aka "Microsoft Silverlight Memory Corruption Vulnerability." **Reference: CVE-2016-3367**	http://technet.microsoft.com/en-us/security/bulletin/ms16-109	A-MIC-SILVE-210916/161
Visio *Microsoft Visio is a diagramming and vector graphics application and is part of the Microsoft Office family.*					
Denial of Service; Overflow Memory Corruption	2016-09-14	9.3	Microsoft Visio 2016 allows remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3364**	http://technet.microsoft.com/en-us/security/bulletin/ms16-107	A-MIC-VISIO-210916/162
MISP-project					
Malware Information Sharing Platform *Malware Information Sharing Platform (MISP) allows organizations to share information about malware and their indicators.*					
NA	2016-09-03	7.5	Malware Information Sharing Platform (MISP) before 2.3.90 allows remote attackers to conduct PHP object injection attacks via crafted serialized data,	https://www.circl.lu/advisory/CVE-2015-5721/	A-MIS-MALWA-210916/163

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

			related to TemplatesController.php and populate_event_from_template_attributes.ctp. **Reference: CVE-2015-5721**		
Cross-site scripting	2016-09-03	4.3	Multiple cross-site scripting (XSS) vulnerabilities in the template-creation feature in Malware Information Sharing Platform (MISP) before 2.3.90 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) add.ctp, (2) edit.ctp, and (3) ajaxification.js. **Reference: CVE-2015-5720**	https://www.circl.lu/advisory/CVE-2015-5720/	A-MIS-MALWA-210916/164
NA	2016-09-03	10	app/Controller/TemplatesController.php in Malware Information Sharing Platform (MISP) before 2.3.92 does not properly restrict filenames under the tmp/files/ directory, which has unspecified impact and attack vectors. **Reference: CVE-2015-5719**	https://www.circl.lu/advisory/CVE-2015-5719/	A-MIS-MALWA-210916/165
Navis					
Webaccess *Navis WebAccess is a web-based application that provides all parties across the terminal with an easy-to-use web browser interface for accessing a wealth of transaction data that was previously inaccessible from outside the terminal.*					
Execute Code; SQL Injection	2016-08-22	7.5	SQL injection vulnerability in news pages in Cargotec Navis WebAccess before 2016-08-10 allows remote attackers to execute	https://ics-cert.us-cert.gov/advisories/ICSA-16-	A-NAV-WEBAC-210916/166

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

			arbitrary SQL commands via unspecified vectors. **Reference: CVE-2016-5817**	231-01	
Netapp					
Clustered Data Ontap *Ontap data management software created to unify your storage infrastructure.*					
Gain Information	2016-08-31	4	NetApp Clustered Data ONTAP before 8.2.4P4 and 8.3.x before 8.3.2P2 allows remote authenticated users to obtain sensitive cluster and tenant information via unspecified vectors. **Reference: CVE-2016-3064**	http://kb.netapp.com/support/index?page=content&id=9010099	A-NET-CLUST-210916/167
On-command System Manager *NetApp On-Command System Manager, which provides fast, simple configuration and management for NetApp FAS data storage systems*					
Denial of Service	2016-09-01	4	NetApp OnCommand System Manager 8.3.x before 8.3.2P5 allows remote authenticated users to cause a denial of service via unspecified vectors. **Reference: CVE-2016-5047**	http://kb.netapp.com/support/index?page=content&id=9010100	A-NET-ONCOM-210916/168
PHP					
PHP *PHP is a server scripting language and a powerful tool for making dynamic and interactive Web pages.*					
Denial of Service; Overflow	2016-09-11	7.5	ext/curl/interface.c in PHP 7.x before 7.0.10 does not work around a libcurl integer overflow, which allows remote attackers to cause a denial of service (allocation error and heap-based buffer overflow) or possibly have unspecified other impact via a long string that is	http://www.php.net/ChangeLog-7.php	A-PHP-PHP-210916/169

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

			mishandled in a curl_escape call. **Reference: CVE-2016-7134**		
Denial of Service; Overflow	2016-09-11	6.8	Zend/zend_alloc.c in PHP 7.x before 7.0.10, when open_basedir is enabled, mishandles huge realloc operations, which allows remote attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact via a long pathname. **Reference: CVE-2016-7133**	http://www.php.net/ChangeLog-7.php	A-PHP-PHP-210916/170
Denial of Service	2016-09-11	5	ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a stray element inside a boolean element, leading to incorrect pop processing. **Reference: CVE-2016-7132**	https://github.com/php/php-src/commit/a14fdb9746262549bbbb96abb87338bacd147e1b?w=1	A-PHP-PHP-210916/171
Denial of Service	2016-09-11	5	ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified	https://github.com/php/php-src/commit/a14fdb9746262549bbbb96abb87338b	A-PHP-PHP-210916/172

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

			other impact via a malformed wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a tag that lacks a < (less than) character. **Reference: CVE-2016-7131**	acd147e1b?w=1	
Denial of Service	2016-09-11	5	The php_wddx_pop_element function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid base64 binary value, as demonstrated by a wddx_deserialize call that mishandles a binary element in a wddxPacket XML document. **Reference: CVE-2016-7130**	https://github.com/php/php-src/commit/698a691724c0a949295991e5df091ce16f899e02?w=1	A-PHP-PHP-210916/173
Denial of Service	2016-09-11	7.5	The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx_deserialize call	https://github.com/php/php-src/commit/426aeb2808955ee3d3f52e0cfb102834cdb836a5?w=1	A-PHP-PHP-210916/174

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

			that mishandles a dateTime element in a wddxPacket XML document. **Reference: CVE-2016-7129**		
Gain Information	2016-09-11	5	The exif_process_IFD_in_TIFF function in ext/exif/exif.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles the case of a thumbnail offset that exceeds the file size, which allows remote attackers to obtain sensitive information from process memory via a crafted TIFF image. **Reference: CVE-2016-7128**	https://github.com/php/php-src/commit/6dbb1ee46b5f4725cc6519abf91e512a2a10dfed?w=1	A-PHP-PHP-210916/175
Denial of Service	2016-09-11	7.5	The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments. **Reference: CVE-2016-7127**	https://bugs.php.net/bug.php?id=72730	A-PHP-PHP-210916/176
Denial of Service	2016-09-11	7.5	The imagetruecolortopalette function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate the number of colors, which	https://bugs.php.net/bug.php?id=72697	A-PHP-PHP-210916/177

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

			allows remote attackers to cause a denial of service (select_colors allocation error and out-of-bounds write) or possibly have unspecified other impact via a large value in the third argument. **Reference: CVE-2016-7126**		
NA	2016-09-11	5	ext/session/session.c in PHP before 5.6.25 and 7.x before 7.0.10 skips invalid session names in a way that triggers incorrect parsing, which allows remote attackers to inject arbitrary-type session data by leveraging control of a session name, as demonstrated by object injection. **Reference: CVE-2016-7125**	https://bugs.php.net/bug.php?id=72681	A-PHP-PHP-210916/178
Denial of Service	2016-09-11	7.5	ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call. **Reference: CVE-2016-7124**	https://bugs.php.net/bug.php?id=72663	A-PHP-PHP-210916/179
Python					
Python *Python is an easy to learn, powerful programming language. It has efficient high-level data structures and a simple but effective approach to object-oriented.*					

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

NA	2016-09-02	4.3	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL. **Reference: CVE-2016-5699**	https://hg.python.org/cpython/rev/bf3e1c9b80e9	A-PYT-PYTHO-210916/180
Overflow	2016-09-02	10	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-based buffer overflow. **Reference: CVE-2016-5636**	https://hg.python.org/cpython/raw-file/v2.7.12/Misc/NEWS	A-PYT-PYTHO-210916/181
Bypass	2016-09-02	5.8	The smtplib library in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 does not return an error when StartTLS fails, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack." **Reference: CVE-2016-**	https://hg.python.org/cpython/rev/d590114c2394	A-PYT-PYTHO-210916/182

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

			0772		
Readydesk					
Readydesk *ReadyDesk is a completely web based help desk software solution that has powerful features to meet the demands of businesses of any size.*					
NA	2016-08-26	4.6	ReadyDesk 9.1 allows local users to determine cleartext SQL Server credentials by reading the SQL_Config.aspx file and decrypting data with a hardcoded key in the ReadyDesk.dll file. **Reference: CVE-2016-5683**	http://www.kb.cert.org/vuls/id/294272	A-REA-READY-210916/183
Execute Code	2016-08-26	7.5	Unrestricted file upload vulnerability in chat/sendfile.aspx in ReadyDesk 9.1 allows remote attackers to execute arbitrary code by uploading and requesting a .aspx file. **Reference: CVE-2016-5050**	http://www.kb.cert.org/vuls/id/294272	A-REA-READY-210916/184
Directory Traversal	2016-08-26	5	Directory traversal vulnerability in chat/openattach.aspx in ReadyDesk 9.1 allows remote attackers to read arbitrary files via a .. (dot dot) in the SESID parameter in conjunction with a filename in the	http://www.kb.cert.org/vuls/id/294272	A-REA-READY-210916/185

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

			FNAME parameter. **Reference: CVE-2016-5049**		
Execute Code; SQL Injection	2016-08-26	7.5	SQL injection vulnerability in chat/staff/default.aspx in ReadyDesk 9.1 allows remote attackers to execute arbitrary SQL commands via the user name field. **Reference: CVE-2016-5048**	http://www.kb.cert.org/vuls/id/294272	A-REA-READY-210916/186
Redhat					
Cloudforms *CloudForms gives you choice and flexibility while providing a unified and consistent set of management capabilities across*					
Execute Code	2016-08-26	6.5	The web UI in Red Hat CloudForms 4.1 allows remote authenticated users to execute arbitrary code via vectors involving "Lack of field filters." **Reference: CVE-2016-5383**	NA	A-RED-CLOUD-210916/187
Jboss Bpm Suite *Red Hat JBoss BPM Suite is the JBoss platform for Business Process Management (BPM). It enables enterprise business and IT users to document, simulate, manage, automate and monitor business processes and policies.*					
Bypass; Cross Site Request Forgery	2016-09-07	6.8	The dashbuilder in Red Hat JBoss BPM Suite 6.3.2 does not properly handle CSRF tokens generated during an active session and includes them in query strings, which makes easier for remote attackers to (1) bypass CSRF protection mechanisms or (2) conduct cross-site request forgery (CSRF) attacks by obtaining an old token. **Reference: CVE-2016-7034**	https://bugzilla.redhat.com/show_bug.cgi?id=1373347	A-RED-JBOSS-210916/188

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

Cross-site scripting	2016-09-07	4.3	Multiple cross-site scripting (XSS) vulnerabilities in the admin pages in dashbuilder in Red Hat JBoss BPM Suite 6.3.2 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-7033**	https://bugzilla.redhat.com/show_bug.cgi?id=1373344	A-RED-JBOSS-210916/189
Gain Information	2016-09-07	5	Red Hat JBoss BPM Suite 6.3.x does not include the HTTPOnly flag in a Set-Cookie header for session cookies, which makes it easier for remote attackers to obtain potentially sensitive information via script access to the cookies. **Reference: CVE-2016-6344**	https://bugzilla.redhat.com/show_bug.cgi?id=1371807	A-RED-JBOSS-210916/190
Jboss Operations Network *JBoss Operations Network simplifies developing, testing, deploying and monitoring your JBoss solutions and the applications running on it .*					
Gain Privileges	2016-09-07	6.5	The web console in Red Hat JBoss Operations Network (JON) before 3.3.7 does not properly authorize requests to add users with the super user role, which allows remote authenticated users to gain admin privileges via a crafted POST request. **Reference: CVE-2016-5422**	NA	A-RED-JBOSS-210916/191
Resteasy *RESTEasy is a JBoss project that provides various frameworks to help you build RESTful Web Services and RESTful Java applications.*					

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

Denial of Service	2016-09-07	5	RESTEasy enables GZIPInterceptor, which allows remote attackers to cause a denial of service via unspecified vectors. **Reference: CVE-2016-6346**	https://bugzilla.redhat.com/show_bug.cgi?id=1372120	A-RED-RESTE-210916/192
Gain Information	2016-09-07	4	RESTEasy allows remote authenticated users to obtain sensitive information by leveraging "insufficient use of random values" in async jobs. **Reference: CVE-2016-6345**	https://bugzilla.redhat.com/show_bug.cgi?id=1372117	A-RED-RESTE-210916/193
Rubyonrails					
Ruby On Rails *Ruby on Rails is open source software to building web application.*					
Bypass	2016-09-07	5	Action Record in Ruby on Rails 4.2.x before 4.2.7.1 does not properly consider differences in parameter handling between the Active Record component and the JSON implementation, which allows remote attackers to bypass intended database-query restrictions and perform NULL checks or trigger missing WHERE clauses via a crafted request, as demonstrated by certain "[nil]" values, a related issue to CVE-2012-2660, CVE-2012-2694, and CVE-2013-0155. **Reference: CVE-2016-6317**	http://weblog.rubyonrails.org/2016/8/11/Rails-5-0-0-1-4-2-7-2-and-3-2-22-3-have-been-released/	A-RUB-RUBY -210916/194
Siemens					

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

En100 Ethernet Module Firmware *Siemens released firmware updates for EN100 Ethernet module included in SIPROTEC 4 and SIPROTEC Compact devices.*					
Bypass	2016-09-05	9	The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain administrative access via unspecified HTTP traffic during an authenticated session. **Reference: CVE-2016-7114**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-630413.pdf	A-SIE-EN100-210916/195
Denial of Service	2016-09-05	7.8	The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to cause a denial of service (defect-mode transition) via crafted HTTP packets. **Reference: CVE-2016-7113**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-630413.pdf	A-SIE-EN100-210916/196
Bypass	2016-09-05	10	The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain administrative access via unspecified HTTP traffic. **Reference: CVE-2016-7112**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-630413.pdf	A-SIE-EN100-210916/197
The Foreman					
Foreman *Foreman has deep integration to configuration management software, with Puppet, Chef, Salt and other solutions through plugins, which allows users to automate repetitive tasks, deploy applications, and manage change to deployed servers.*					
Cross-site	2016-08-	3.5	Cross-site scripting (XSS)	https://the	A-THE-

scripting	19		vulnerability in app/assets/javascripts/host_edit_interfaces.js in Foreman before 1.12.2 allows remote authenticated users to inject arbitrary web script or HTML via the network interface device identifier in the host interface form. **Reference: CVE-2016-6320**	foreman.org/security.html#2016-6320	FOREM-210916/198
Cross-site scripting	2016-08-19	4.3	Cross-site scripting (XSS) vulnerability in app/helpers/form_helper.rb in Foreman before 1.12.2, as used by Remote Execution and possibly other plugins, allows remote attackers to inject arbitrary web script or HTML via the label parameter. **Reference: CVE-2016-6319**	https://bugzilla.redhat.com/show_bug.cgi?id=1365815	A-THE-FOREM-210916/199
Gain Information	2016-08-19	2.1	Foreman before 1.11.4 and 1.12.x before 1.12.1 allow remote authenticated users with the view_hosts permission containing a filter to obtain sensitive network interface information via a request to API routes beneath "hosts," as demonstrated by a GET request to api/v2/hosts/secrethost/interfaces. **Reference: CVE-2016-5390**	https://bugzilla.redhat.com/show_bug.cgi?id=1355728	A-THE-FOREM-210916/200
Gain Information	2016-08-19	3.5	Foreman before 1.11.4 and 1.12.x before 1.12.1 does not properly restrict	https://theforeman.org/security	A-THE-FOREM-210916/20

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

			access to preview provisioning templates, which allows remote authenticated users with permission to view some hosts to obtain sensitive host configuration information via a URL with a hostname. **Reference: CVE-2016-4995**	.html#2016-4995	1
Bypass	2016-08-19	6.5	The (1) Organization and (2) Locations APIs and UIs in Foreman before 1.11.4 and 1.12.x before 1.12.0-RC3 allow remote authenticated users to bypass organization and location restrictions and (a) read, (b) edit, or (c) delete arbitrary organizations or locations via unspecified vectors. **Reference: CVE-2016-4475**	https://theforeman.org/security.html#2016-4475	A-THE-FOREM-210916/202
Bypass	2016-08-19	6	The (1) Organization and (2) Locations APIs in Foreman before 1.11.3 and 1.12.x before 1.12.0-RC1 allow remote authenticated users with unlimited filters to bypass organization and location restrictions and read or modify data for an arbitrary organization by leveraging knowledge of the id of that organization. **Reference: CVE-2016-4451**	http://projects.theforeman.org/issues/15182	A-THE-FOREM-210916/203
Tryton					
Tryton *Tryton is a three-tier high-level general purpose computer application platform on*					

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

top of which is built an Enterprise resource planning (ERP) business solution.					
Gain Information	2016-09-07	4	file_open in Tryton before 3.2.17, 3.4.x before 3.4.14, 3.6.x before 3.6.12, 3.8.x before 3.8.8, and 4.x before 4.0.4 allow remote authenticated users with certain permissions to read arbitrary files via the name parameter or unspecified other vectors. **Reference: CVE-2016-1242**	https://bugs.tryton.org/issue5808	A-TRY-TRYTO-210916/204
Gain Information	2016-09-07	3.5	Tryton 3.x before 3.2.17, 3.4.x before 3.4.14, 3.6.x before 3.6.12, 3.8.x before 3.8.8, and 4.x before 4.0.4 allow remote authenticated users to discover user password hashes via unspecified vectors. **Reference: CVE-2016-1241**	https://bugs.tryton.org/issue5795	A-TRY-TRYTO-210916/205
Ultravnc					
Repeater *The repeater acts like a proxy, sitting in the middle between the server and viewer. All data for the session is passed through the repeater meaning that the viewer and server can both be behind a NAT firewall, without having to worry about forwarding ports or anything else (providing the repeater is visible to both viewer and server).*					
NA	2016-08-25	5	UltraVNC Repeater before 1300 does not restrict destination IP addresses or TCP ports, which allows remote attackers to obtain open-proxy functionality by using a :: substring in between the IP address and port number. **Reference: CVE-2016-5673**	http://www.kb.cert.org/vuls/id/BLUU-A9WQVP	A-ULT-REPEA-210916/206

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

Vbulletin					
Vbulletin *vBulletin is leading application of forum and community publishing software.*					
Execute Code; SQL Injection	2016-08-30	7.5	SQL injection vulnerability in forumrunner/includes/moderation.php in vBulletin before 4.2.2 Patch Level 5 and 4.2.3 before Patch Level 1 allows remote attackers to execute arbitrary SQL commands via the postids parameter to forumrunner/request.php, as exploited in the wild in July 2016. **Reference: CVE-2016-6195**	http://www.vbulletin.org/forum/showthread.php?t=322848	A-VBU-VBULL-210916/207
NA	2016-09-01	5	The media-file upload feature in vBulletin before 3.8.7 Patch Level 6, 3.8.8 before Patch Level 2, 3.8.9 before Patch Level 1, 4.x before 4.2.2 Patch Level 6, 4.2.3 before Patch Level 2, 5.x before 5.2.0 Patch Level 3, 5.2.1 before Patch Level 1, and 5.2.2 before Patch Level 1 allows remote attackers to conduct SSRF attacks via a crafted URL that results in a Redirection HTTP status code. **Reference: CVE-2016-6483**	http://www.vbulletin.com/forum/forum/vbulletin-announcements/vbulletin-announcements_aa/4349551-security-patch-vbulletin-5-2-0-5-2-1-5-2-2	A-VBU-VBULL-210916/208
Vmware					
Identity Manger;Vrealize Automation *An identity management system refers to an information system, or to a set of technologies that can be used for enterprise or cross-network identity management.*					

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

NA	2016-08-30	7.2	VMware Identity Manager 2.x before 2.7 and vRealize Automation 7.0.x before 7.1 allow local users to obtain root access via unspecified vectors. **Reference: CVE-2016-5335**	http://www.vmware.com/security/advisories/VMSA-2016-0013.html	A-VMW-IDENT-210916/209
Execute Code	2016-08-30	7.5	VMware vRealize Automation 7.0.x before 7.1 allows remote attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-5336**	http://www.vmware.com/security/advisories/VMSA-2016-0013.html	A-VMW-VREAL-210916/210
Vrealize Log Insight *vRealize Log Insight delivers heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics and broad third-party extensibility, providing deep operational visibility and faster troubleshooting.*					
Directory Traversal	2016-08-30	5	Directory traversal vulnerability in VMware vRealize Log Insight 2.x and 3.x before 3.6.0 allows remote attackers to read arbitrary files via unspecified vectors. **Reference: CVE-2016-5332**	http://www.vmware.com/security/advisories/VMSA-2016-0011.html	A-VMW-VREAL-210916/211
Watchguard					
Rapidstream:NA					
Execute Code; Gain Info	2016-08-24	7.2	WatchGuard RapidStream appliances allow local users to gain privileges and execute arbitrary commands via a crafted ifconfig command, aka ESCALATEPLOWMAN. **Reference: CVE-2016-7089**	NA	A-WAT-RAPID-210916/212
Wireshark					
Wireshark *Wireshark is a network protocol analyzer for Unix and Windows.*					

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

Denial of Service	2016-09-09	4.3	epan/dissectors/packet-ipmi-trace.c in the IPMI trace dissector in Wireshark 2.x before 2.0.6 does not properly consider whether a string is constant, which allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted packet. **Reference: CVE-2016-7180**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12782	A-WIR-WIRES-210916/213
Denial of Service; Overflow	2016-09-09	4.3	Stack-based buffer overflow in epan/dissectors/packet-catapult-dct2000.c in the Catapult DCT2000 dissector in Wireshark 2.x before 2.0.6 allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference: CVE-2016-7179**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=3b97fbddc23c065727b0147aab52a27c4aadffe7	A-WIR-WIRES-210916/214
Denial of Service	2016-09-09	4.3	epan/dissectors/packet-umts_fp.c in the UMTS FP dissector in Wireshark 2.x before 2.0.6 does not ensure that memory is allocated for certain data structures, which allows remote attackers to cause a denial of service (invalid write access and application crash) via a crafted packet. **Reference: CVE-2016-7178**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=315bba7c645b75af24215c6303d187b188610bba	A-WIR-WIRES-210916/215
Denial of Service; Overflow	2016-09-09	4.3	epan/dissectors/packet-catapult-dct2000.c in the Catapult DCT2000	https://code.wireshark.org/revie	A-WIR-WIRES-210916/21

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

			dissector in Wireshark 2.x before 2.0.6 does not restrict the number of channels, which allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted packet. **Reference: CVE-2016-7177**	w/gitweb?p=wireshark.git;a=commit;h=2e37b271c473e1cbd01d62ebe1f3b011fc9fe638	6
Denial of Service; Overflow	2016-09-09	4.3	epan/dissectors/packet-h225.c in the H.225 dissector in Wireshark 2.x before 2.0.6 calls snprintf with one of its input buffers as the output buffer, which allows remote attackers to cause a denial of service (copy overlap and application crash) via a crafted packet. **Reference: CVE-2016-7176**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=6d8261994bb928b7e80e3a2478a3d939ea1ef373	A-WIR-WIRES-210916/217
Denial of Service	2016-09-09	4.3	epan/dissectors/packet-qnet6.c in the QNX6 QNET dissector in Wireshark 2.x before 2.0.6 mishandles MAC address data, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet. **Reference: CVE-2016-7175**	https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=1396f6ad55178f6b81cc1a65f9cb37b2d99aebf	A-WIR-WIRES-210916/218
Zimbra Collaboration Server					
Zimbra Collaboration Server *Zimbra is an enterprise-class email, calendar and collaboration solution built for the cloud, both public and private. With a redesigned browser-based interface, Zimbra offers the most innovative messaging experience available today, connecting end users to the information and activity in their personal clouds.*					

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

Cross-site scripting	2016-08-29	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Zimbra Collaboration before 8.7.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-5721**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories	A-ZIM-ZIMBR-210916/219
F5/F5					
Big-ip Access Policy Manager; Big-ip Advanced Firewall Manager; Big-ip Analytics; Big-ip Application Acceleration Manager; Big-ip Application Security Manager; Big-ip Domain Name System; Big-ip Edge Gateway; Big-ip Global Traffic Manager; Big-ip Link Controller; Big-ip Local Traffic Manager; Big-ip Policy Enforcement Manager; Big-ip Wan Optimization Manager; Big-ip Webaccelerator; Big-ip Websafe/Big-ip Protocol Security Manager *A central policy control point delivers access based on context and is critical to managing a scalable, secure, and dynamic environment; BIG-IP Advanced Firewall Manager (AFM) delivers the most effective network-level security for enterprises and service providers. Whether on-premises or in an SDDC environment, BIG-IP AFM tracks the state of network sessions, maintains application awareness, and uniquely mitigates attacks based on more attack details than traditional network firewalls; Big-ip Analytics provides detailed metrics such as transactions per second, server and client latency, request and response throughput, and sessions. Big-ip Application Acceleration Manager of data center, transport, and application optimizations in Application Acceleration Manager (AAM) overcomes WAN latency, maximizes server capacity, and speeds application response times; BIG-IP Application Security Manager (ASM) enables organizations to protect against OWASP top 10 threats, application vulnerabilities, and zero-day attacks; BIG-IP DNS hyperscales and secures your infrastructure during high query volumes and DDoS attacks to keep your global apps online;F5 BIG-IP Edge Gateway is an accelerated remote access solution that brings together SSL VPN, security, application acceleration, and availability services;BIG-IP Global Traffic Manager distributes DNS and user application requests based on business policies, data center and cloud service conditions, user location, and application performance; WAN Optimization Manager (WOM) overcomes network and application issues on the WAN to ensure that application performance, data replication; Protocol Security Module provides advanced protocol security, and ensures compliance for common internet protocols. The Protocol Security Module protects your web servers and FTP servers, masks sensitive data, blocks spam.*					

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

NA	2016-08-19	5	The default configuration of the IPsec IKE peer listener in F5 BIG-IP LTM, Analytics, APM, ASM, and Link Controller 11.2.1 before HF16, 11.4.x, 11.5.x before 11.5.4 HF2, 11.6.x before 11.6.1, and 12.x before 12.0.0 HF2; BIG-IP AAM, AFM, and PEM 11.4.x, 11.5.x before 11.5.4 HF2, 11.6.x before 11.6.1, and 12.x before 12.0.0 HF2; BIG-IP DNS 12.x before 12.0.0 HF2; BIG-IP Edge Gateway, WebAccelerator, and WOM 11.2.1 before HF16; BIG-IP GTM 11.2.1 before HF16, 11.4.x, 11.5.x before 11.5.4 HF2, and 11.6.x before 11.6.1; and BIG-IP PSM 11.4.0 through 11.4.1 improperly enables the anonymous IPsec IKE peer configuration object, which allows remote attackers to establish an IKE Phase 1 negotiation and possibly conduct brute-force attacks against Phase 2 negotiations via unspecified vectors. **Reference: CVE-2016-5736**	https://support.f5.com/kb/en-us/solutions/public/k/10/sol10133477.html	A-F5/-BIG-I-210916/220
Denial of Service	2016-08-26	5	Virtual servers in F5 BIG-IP systems 11.2.1 HF11 through HF15, 11.4.1 HF4 through HF10, 11.5.3 through 11.5.4, 11.6.0 HF5 through HF7, and 12.0.0, when configured with a TCP profile, allow remote attackers to cause	https://support.f5.com/kb/en-us/solutions/public/k/19/sol19784568.html	A-F5/-BIG-I-210916/221

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

			a denial of service (Traffic Management Microkernel restart) via crafted network traffic. **Reference: CVE-2016-5023**		
Gain Information	2016-08-26	4	The Configuration utility in F5 BIG-IP systems 11.0.x, 11.1.x, 11.2.x before 11.2.1 HF16, 11.3.x, 11.4.x before 11.4.1 HF10, 11.5.x before 11.5.4 HF2, 1.6.x before 11.6.1, and 12.0.0 before HF1 allows remote administrators to read Access Policy Manager (APM) access logs via unspecified vectors. **Reference: CVE-2016-1497**	https://support.f5.com/kb/en-us/solutions/public/k/31/sol31925518.html	A-F5/-BIG-I-210916/222
Denial of Service	2016-09-07	5	The RESOLV::lookup iRule command in F5 BIG-IP LTM, APM, ASM, and Link Controller 10.2.1 through 10.2.4, 11.2.1, 11.4.x, 11.5.x before 11.5.4 HF2, 11.6.x before 11.6.1, and 12.0.0 before HF3; BIG-IP AAM, AFM, and PEM 11.4.x, 11.5.x before 11.5.4 HF2, 11.6.x before 11.6.1, and 12.0.0 before HF3; BIG-IP Analytics 11.2.1, 11.4.x, 11.5.x before 11.5.4 HF2, 11.6.x before 11.6.1, and 12.0.0 before HF3; BIG-IP DNS 12.0.0 before HF3; BIG-IP Edge Gateway, WebAccelerator, and WOM 10.2.1 through 10.2.4 and 11.2.1; BIG-IP GTM 10.2.1 through	https://support.f5.com/kb/en-us/solutions/public/k/52/sol52638558.html	A-F5/-BIG-I-210916/223

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

			10.2.4, 11.2.1, 11.4.x, 11.5.x before 11.5.4 HF2, and 11.6.x before 11.6.1; and BIG-IP PSM 10.2.1 through 10.2.4 and 11.4.0 through 11.4.1 allows remote DNS servers to cause a denial of service (CPU consumption or Traffic Management Microkernel crash) via a crafted PTR response. **Reference: CVE-2016-6876**		
Denial of Service	2016-09-07	7.5	F5 BIG-IP LTM, Analytics, APM, ASM, and Link Controller 11.2.x before 11.2.1 HF16, 11.3.x, 11.4.x, 11.5.x before 11.5.4 HF2, 11.6.x before 11.6.1 HF1, and 12.x before 12.0.0 HF3; BIG-IP AAM, AFM, and PEM 11.4.x, 11.5.x before 11.5.4 HF2, 11.6.x before 11.6.1 HF1, and 12.x before 12.0.0 HF3; BIG-IP DNS 12.x before 12.0.0 HF3; BIG-IP Edge Gateway, WebAccelerator, and WOM 11.2.x before 11.2.1 HF16 and 11.3.0; BIG-IP GTM 11.2.x before 11.2.1 HF16, 11.3.x, 11.4.x, 11.5.x before 11.5.4 HF2, and 11.6.x before 11.6.1 HF1; BIG-IP PSM 11.2.x before 11.2.1 HF16, 11.3.x, and 11.4.0 through 11.4.1; Enterprise Manager 3.1.1; BIG-IQ Cloud and Security 4.0.0 through 4.5.0; BIG-IQ Device 4.2.0 through 4.5.0; BIG-IQ ADC 4.5.0;	https://support.f5.com/kb/en-us/solutions/public/k/06/sol06045217.html	A-F5/-BIG-I-210916/224

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

			BIG-IQ Centralized Management 5.0.0; BIG-IQ Cloud and Orchestration 1.0.0; and iWorkflow 2.0.0, when Packet Filtering is enabled on virtual servers and possibly self IP addresses, allow remote attackers to cause a denial of service (Traffic Management Microkernel restart) and possibly have unspecified other impact via crafted network traffic. **Reference: CVE-2016-5022**		
Gain Privileges	2016-08-19	8.5	The Configuration utility in F5 BIG-IP LTM, Analytics, APM, ASM, GTM, and Link Controller 11.x before 11.2.1 HF16, 11.3.x, 11.4.x before 11.4.1 HF10, 11.5.x before 11.5.4, and 11.6.x before 11.6.1; BIG-IP AAM 11.4.x before 11.4.1 HF10, 11.5.x before 11.5.4, and 11.6.x before 11.6.1; BIG-IP AFM and PEM 11.3.x, 11.4.x before 11.4.1 HF10, 11.5.x before 11.5.4, and 11.6.x before 11.6.1; BIG-IP Edge Gateway, WebAccelerator, and WOM 11.x before 11.2.1 HF16 and 11.3.0; and BIG-IP PSM 11.x before 11.2.1 HF16, 11.3.x, and 11.4.x before 11.4.1 HF10 allows remote authenticated users with certain permissions to gain privileges by leveraging	https://support.f5.com/kb/en-us/solutions/public/k/12/sol12401251.html	A-F5/-BIG-I-210916/225

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

			an Access Policy Manager customization configuration section that allows file uploads. **Reference: CVE-2015-8022**		
Cisco					
Adaptive Security Appliance Software;Firepower Services Software For Asa;Firepower Threat Defense Software/Asa 1000v Cloud Firewall Software;Pix Firewall *Cisco ASA Software delivers enterprise-class security capabilities for the ASA security family in a variety of form factors;Beat sophisticated cyber attacks with a superior security appliance, industry's first threat-focused next-generation firewall (NGFW), the ASA 5500-X Series; Firepower Threat Defense Software network security appliances are based on Snort, an open-source intrusion detection system (IDS);Cisco PIX (Private Internet eXchange) was a popular IP firewall and network address translation (NAT) appliance.*					
Execute Code; Overflow	2016-08-18	8.5	Buffer overflow in Cisco Adaptive Security Appliance (ASA) Software through 9.4.2.3 on ASA 5500, ASA 5500-X, ASA Services Module, ASA 1000V, ASAv, Firepower 9300 ASA Security Module, PIX, and FWSM devices allows remote authenticated users to execute arbitrary code via crafted IPv4 SNMP packets, aka Bug ID CSCva92151 or EXTRABACON. **Reference: CVE-2016-6366**	http://tools.cisco.com/security/center/viewErp.x?alertId=ERP-56516	A-CIS-ADAPT-210916/226
Cisco;Openssl;Python;Redhat/Redhat					
Content Security Management Appliance/Openssl/Python/Jboss Enterprise Application Platform; Jboss Enterprise Web Server; Jboss Web Server/Enterprise Linux *The Cisco Content Security Management Appliance (SMA) centralizes management and reporting functions across multiple Cisco email and web security appliances; 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;*					

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

JBoss Web Server is an enterprise ready web server designed for medium and large applications; Red Hat JBoss Middleware provides cloud-native services, from developer tools to data management, so you can develop applications faster, smarter, and more flexibly.					
Gain Information	2016-08-31	5	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack. **Reference: CVE-2016-2183**	https://www.openssl.org/blog/blog/2016/08/24/sweet32/	A-CIS-CONTE-210916/227
Collectd/Debian					
Collectd/Debian Linux *Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License, and packaged by a group of individuals called the Debian Project.*					
Denial of Service; Execute Code; Overflow	2016-08-19	6.4	Heap-based buffer overflow in the parse_packet function in network.c in collectd before 5.4.3 and 5.x before 5.5.2 allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted network packet. **Reference: CVE-2016-6254**	http://collectd.org/news.shtml	A-COL-COLLE-210916/228
Cracklib Project/Novell					

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

Cracklib/Leap *CrackLib tests passwords to determine whether they match certain security-oriented characteristics*					
Denial of Service; Overflow ; Gain Privileges	2016-09-07	7.2	Stack-based buffer overflow in the FascistGecosUser function in lib/fascist.c in cracklib allows local users to cause a denial of service (application crash) or gain privileges via a long GECOS field, involving longbuffer. **Reference: CVE-2016-6318**	NA	A-CRA-CRACK-210916/229
Dbd-mysql Project/Debian					
Dbd-mysql/Debian Linux: NA					
NA	2016-08-19	10	Use-after-free vulnerability in the my_login function in DBD::mysql before 4.033_01 allows attackers to have unspecified impact by leveraging a call to mysql_errno after a failure of my_login. **Reference: CVE-2015-8949**	https://github.com/perl5-dbi/DBD-mysql/pull/45	A-DBD-DBD-M-210916/230
Microsoft					
Edge/Windows 10;Windows 8.1;Windows Rt 8.1;Windows Server 2012 *Windows is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems.Windows Server series is Microsoft Windows server line of operating systems.*					
Gain Information	2016-09-14	4.3	The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka "PDF Library Information Disclosure	NA	A-MIC-EDGE/-210916/231

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

			Vulnerability," a different vulnerability than CVE-2016-3370. **Reference: CVE-2016-3374**		
Gain Information	2016-09-14	4.3	The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka "PDF Library Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3374. **Reference: CVE-2016-3370**		A-MIC-EDGE/-210916/232
Internet Explorer/Windows 10;Windows 7;Windows 8.1;Windows Rt 8.1;Windows Server 2008;Windows Server 2012;Windows Vista *Internet Explorer is a Web Browser/ Windows is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems; Windows Server series is Microsoft Windows server line of operating systems.*					
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-14	7.6	The OLE Automation mechanism and VBScript scripting engine in Microsoft Internet Explorer 9 through 11, 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, 1511, and 1607 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a	NA	A-MIC-INTER-210916/233

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

			crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." **Reference: CVE-2016-3375**		
Netgear/Nuuo					
Readynas Surveillance/Nvrmini 2 *The Netgear ReadyNAS line of SOHO and small business NAS systems offers a robust set of management features.*					
Execute Code; Overflow	2016-08-31	9	Stack-based buffer overflow in cgi-bin/cgi_main in NUUO NVRmini 2 1.7.6 through 3.0.0 and NETGEAR ReadyNAS Surveillance 1.1.2 allows remote authenticated users to execute arbitrary code via the sn parameter to the transfer_license command. **Reference: CVE-2016-5680**	http://www.kb.cert.org/vuls/id/856152	A-NET-READY-210916/234
Execute Code	2016-08-31	9	cgi-bin/cgi_main in NUUO NVRmini 2 1.7.6 through 3.0.0 and NETGEAR ReadyNAS Surveillance 1.1.2 allows remote authenticated users to execute arbitrary commands via shell metacharacters in the sn parameter to the transfer_license command. **Reference: CVE-2016-5679**	http://www.kb.cert.org/vuls/id/856152	A-NET-READY-210916/235
Readynas Surveillance/Nvrmini 2;Nvrsolo *The Netgear ReadyNAS line of SOHO and small business NAS systems offers a robust set of management features.*					
Gain Information	2016-08-31	5	NUUO NVRmini 2 1.7.5 through 3.0.0, NUUO NVRsolo 1.0.0 through 3.0.0, and NETGEAR	http://www.kb.cert.org/vuls/id/856152	A-NET-READY-210916/236

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

			ReadyNAS Surveillance 1.1.1 through 1.4.1 have a hardcoded qwe23622260 password for the nuuoeng account, which allows remote attackers to obtain sensitive information via an __nvr_status___.php request. **Reference: CVE-2016-5677**		
NA	2016-08-31	5	cgi-bin/cgi_system in NUUO NVRmini 2 1.7.5 through 2.x, NUUO NVRsolo 1.7.5 through 2.x, and NETGEAR ReadyNAS Surveillance 1.1.1 through 1.4.1 allows remote attackers to reset the administrator password via a cmd=loaddefconfig action. **Reference: CVE-2016-5676**	http://www.kb.cert.org/vuls/id/856152	A-NET-READY-210916/237
Execute Code	2016-08-31	10	__debugging_center_utils___.php in NUUO NVRmini 2 1.7.5 through 3.0.0, NUUO NVRsolo 1.7.5 through 3.0.0, and NETGEAR ReadyNAS Surveillance 1.1.1 through 1.4.1 allows remote attackers to execute arbitrary PHP code via the log parameter. **Reference: CVE-2016-5674**	http://www.kb.cert.org/vuls/id/856152	A-NET-READY-210916/238
Execute Code	2016-08-31	10	handle_daylightsaving.php in NUUO NVRmini 2 1.7.5 through 3.0.0, NUUO NVRsolo 1.0.0 through 3.0.0, NUUO Crystal 2.2.1	http://www.kb.cert.org/vuls/id/856152	A-NET-READY-210916/239

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

			through 3.2.0, and NETGEAR ReadyNAS Surveillance 1.1.1 through 1.4.1 allows remote attackers to execute arbitrary PHP code via the NTPServer parameter. **Reference: CVE-2016-5675**		
Hardware					
Rockwell Automation					
1766-l32awa;1766-l32awaa;1766-l32bwa;1766-l32bwaa;1766-l32bxb;1766-l32bxba *Rockwell Automation complements the existing MicroLogix family of small programmable logic controllers. MicroLogix 1400 combines the features you demand from MicroLogix 1100, such as EtherNet/IP, online editing, and a built-in LCD, plus provides you with enhanced features, such as higher I/O count, faster High Speed Counter/PTO and enhanced network capabilities*					
NA	2016-08-23	7.5	Rockwell Automation MicroLogix 1400 PLC 1766-L32BWA, 1766-L32AWA, 1766-L32BXB, 1766-L32BWAA, 1766-L32AWAA, and 1766-L32BXBA devices have a hardcoded SNMP community, which makes it easier for remote attackers to load arbitrary firmware updates by leveraging knowledge of this community. **Reference: CVE-2016-5645**	https://ics-cert.us-cert.gov/advisories/ICSA-16-224-01	H-ROC-1766--210916/240
Zmodo					
Zp-ibh-13w;Zp-ne-14-s *Zmodo Zp-ibh-13w high definition wireless IP camera provides a complete, cost-effective network video surveillance solution, ideal for monitoring homes, small offices and retail businesses.*					
NA	2016-08-23	10	ZModo ZP-NE14-S and ZP-IBH-13W devices have a hardcoded root password, which makes it easier for remote attackers to	http://www.kb.cert.org/vuls/id/301735	H-ZMO-ZP-IB-210916/241

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

			obtain access via a TELNET session. **Reference: CVE-2016-5081**		
NA	2016-08-23	5	ZModo ZP-NE14-S and ZP-IBH-13W devices do not enforce a WPA2 configuration setting, which allows remote attackers to trigger association with an arbitrary access point by using a recognized SSID value. **Reference: CVE-2016-5650**	http://www.kb.cert.org/vuls/id/301735	H-ZMO-ZP-IB-210916/242
Ace 4700 Series Application Control Engine Appliance;Ace 4700 Series Application Control Engine Appliance A1;Ace 4700 Series Application Control Engine Appliance A3;Ace 4700 Series Application Control Engine Appliance A4;Ace 4700 Series Application Control Engine Appliance A5/Ace Application Control Engine Module A1;Ace Application Control Engine Module A3;Ace Application Control Engine Module A4;Ace Application Control Engine Module A5 *Cisco Ace Application Control Engine Module Series Routers is a next-generation load-balancing and application-delivery solution. A member of the Cisco family of Data Center*					
Denial of Service	2016-09-12	7.8	Cisco ACE30 Application Control Engine Module through A5 3.3 and ACE 4700 Application Control Engine appliances through A5 3.3 allow remote attackers to cause a denial of service (device reload) via crafted (1) SSL or (2) TLS packets, aka Bug ID CSCvb16317. **Reference: CVE-2016-6399**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160908-ace	H-CIS-ACE4-210916/243
Operating System					
Apple					
Iphone Os *iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware.*					

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

Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-18	9.3	IOMobileFrameBuffer in Apple iOS before 9.3.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4654**	https://support.apple.com/HT207026	O-APP-IPHON-210916/244
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-25	6.8	WebKit in Apple iOS before 9.3.5 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference: CVE-2016-4657**	https://support.apple.com/HT207107	O-APP-IPHON-210916/245
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-25	9.3	The kernel in Apple iOS before 9.3.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4656**	https://support.apple.com/HT207107	O-APP-IPHON-210916/246
Gain Information	2016-08-25	7.1	The kernel in Apple iOS before 9.3.5 allows attackers to obtain sensitive information from memory via a crafted app. **Reference: CVE-2016-4655**	https://support.apple.com/HT207107	O-APP-IPHON-210916/247
Brocade					
Fabric Os *Cisco IOS is network infrastructure software, delivering a seamless integration of technology innovation, business-critical services, and hardware platform support.*					

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

Gain Information	2016-08-22	7.8	HPE FOS before 7.4.1d and 8.x before 8.0.1 on StoreFabric B switches allows remote attackers to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-4376**	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05236212	O-BRO-FABRI-210916/248
Cisco					
IOS:NA					
Gain Information	2016-09-12	5	The PPTP server in Cisco IOS 15.5(3)M does not properly initialize packet buffers, which allows remote attackers to obtain sensitive information from earlier network communication by reading packet data, aka Bug ID CSCvb16274. **Reference: CVE-2016-6398**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160902-ios	O-CIS-IOS-210916/249
Ios Xr *IOS XR is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), used on their high-end Network Converging System(NCS), carrier-grade routers*					
Denial of Service	2016-08-22	7.8	Memory leak in Cisco IOS XR 5.1.x through 5.1.3, 5.2.x through 5.2.5, and 5.3.x through 5.3.2 on ASR 9001 devices allows remote attackers to cause a denial of service (control-plane protocol outage) via crafted fragmented packets, aka Bug ID CSCux26791. **Reference: CVE-2016-6355**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160810-iosxr	O-CIS-IOSX-210916/250
Ip Phone 8800 Series Firmware *The Cisco IP Phone 8800 Series delivers HD video and VoIP communications, and integrates with your mobile device to meet your business needs.*					

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

Denial of Service; Memory Corruption	2016-08-22	7.8	Cisco IP Phone 8800 devices with software 11.0(1) allow remote attackers to cause a denial of service (memory corruption) via a crafted HTTP request, aka Bug ID CSCuz03038. **Reference: CVE-2016-1479**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ipp	O-CIS-IPPH-210916/251
Ip Phone 8800 Series Firmware *The Cisco IP Phone 8800 Series delivers HD video and VoIP communications, and integrates with your mobile device to meet your business needs.*					
Cross-site scripting	2016-08-22	3.5	Cross-site scripting (XSS) vulnerability on Cisco IP Phone 8800 devices with software 11.0 allows remote authenticated users to inject arbitrary web script or HTML via crafted parameters, aka Bug ID CSCuz03024. **Reference: CVE-2016-1476**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160810-ip-phone-8800	O-CIS-IPPH-210916/252
Spa300 Series Ip Phone Firmware;Spa500 Series Ip Phone Firmware *Cisco Spa300 Series Ip Phone Firmware provide traditional features, such as call forwarding, redialing, speed dialing, transferring calls, conference calling and accessing voice mail.*					
Denial of Service	2016-09-11	7.8	The HTTP framework on Cisco SPA300, SPA500, and SPA51x devices allows remote attackers to cause a denial of service (device outage) via a series of malformed HTTP requests, aka Bug ID CSCut67385. **Reference: CVE-2016-1469**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-spa	O-CIS-SPA30-210916/253
Wireless Lan Controller Software;Wireless Lan Controller Software 6.0;Wireless Lan Controller Software 7.0;Wireless Lan Controller Software 7.1;Wireless Lan Controller Software 7.2;Wireless Lan Controller Software 7.4 *Cisco Wireless LAN Controller (WLAN), wireless controller, provides wireless*					

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

performance of all mobile devices, offers limited hotspot coverage.					
Denial of Service	2016-09-11	5.7	Cisco Wireless LAN Controller (WLC) devices before 8.0.140.0, 8.1.x and 8.2.x before 8.2.121.0, and 8.3.x before 8.3.102.0 allow remote attackers to cause a denial of service (device reload) by sending crafted Inter-Access Point Protocol (IAPP) packets and then sending a traffic stream metrics (TSM) information request over SNMP, aka Bug ID CSCuz40221. **Reference: CVE-2016-6375**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160831-wlc-1	O-CIS-WIREL-210916/254
Debian					
Debian Linux *An operating system is the set of basic programs and utilities that make your computer run.*					
Denial of Service	2016-08-31	4.9	fs/fcntl.c in the "aufs 3.2.x+setfl-debian" patch in the linux-image package 3.2.0-4 (kernel 3.2.81-1) in Debian wheezy mishandles F_SETFL fcntl calls on directories, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via standard filesystem operations, as demonstrated by scp from an AUFS filesystem. **Reference: CVE-2016-7118**	http://www.openwall.com/lists/oss-security/2016/08/31/3	O-DEB-DEBIA-210916/255
Fortinet					
Fortianalyzer Firmware;Fortimanager Firmware *FortiClient is fully integrated with FortiGate, FortiManager, and FortiAnalyzer for*					

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

management, deployment, and central logging/reporting					
Cross-site scripting	2016-08-19	4.3	Cross-site scripting (XSS) vulnerability in the Web-UI in Fortinet FortiManager 5.x before 5.0.12 and 5.2.x before 5.2.6 and FortiAnalyzer 5.x before 5.0.13 and 5.2.x before 5.2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-3195**	http://fortiguard.com/advisory/fortimanager-and-fortianalyzer-client-side-xss-vulnerability	O-FOR-FORTI-210916/256
Cross-site scripting	2016-08-19	4.3	Cross-site scripting (XSS) vulnerability in the address added page in Fortinet FortiManager 5.x before 5.0.12 and 5.2.x before 5.2.6 and FortiAnalyzer 5.x before 5.0.13 and 5.2.x before 5.2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-3194**	http://fortiguard.com/advisory/fortimanager-and-fortianalyzer-xss-vulnerability	O-FOR-FORTI-210916/257
Cross-site scripting	2016-08-19	3.5	Cross-site scripting (XSS) vulnerability in the appliance web-application in Fortinet FortiManager 5.x before 5.0.12, 5.2.x before 5.2.6, and 5.4.x before 5.4.1 and FortiAnalyzer 5.x before 5.0.13, 5.2.x before 5.2.6, and 5.4.x before 5.4.1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified	http://fortiguard.com/advisory/fortimanager-and-fortianalyzer-persistent-xss-vulnerability-1	O-FOR-FORTI-210916/258

			vectors. **Reference: CVE-2016-3193**		
Fortios;Fortiswitch *Use FortiGate to provide remote management for FortiSwitch units. The FortiGate requires a one-time configuration task to enable the Switch Controller on it. FortiSwitch Data Center and Secure Access Switches are cost-effective and flexible, and are available in a wide range of models to fit any environment.*					
Execute Code; Overflow	2016-08-24	10	Buffer overflow in the Cookie parser in Fortinet FortiOS 4.x before 4.1.11, 4.2.x before 4.2.13, and 4.3.x before 4.3.9 and FortiSwitch before 3.4.3 allows remote attackers to execute arbitrary code via a crafted HTTP request, aka EGREGIOUSBLUNDER. **Reference: CVE-2016-6909**	http://fortiguard.com/advisory/FG-IR-16-023	O-FOR-FORTI-210916/259
Fortiswitch *FortiSwitch Data Center and Secure Access Switches are cost-effective and flexible, and are available in a wide range of models to fit any environment.*					
Bypass	2016-09-09	10	Fortinet FortiSwitch FSW-108D-POE, FSW-124D, FSW-124D-POE, FSW-224D-POE, FSW-224D-FPOE, FSW-248D-POE, FSW-248D-FPOE, FSW-424D, FSW-424D-POE, FSW-424D-FPOE, FSW-448D, FSW-448D-POE, FSW-448D-FPOE, FSW-524D, FSW-524D-FPOE, FSW-548D, FSW-548D-FPOE, FSW-1024D, FSW-1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink managed mode and upgraded to 3.4.1, might allow remote attackers to	http://fortiguard.com/advisory/fortiswitch-rest-admin-account-exposed-under-specific-conditions	O-FOR-FORTI-210916/260

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

			bypass authentication and gain administrative access via an empty password for the rest_admin account. **Reference: CVE-2016-4573**		
Google					
Android *Android is an OS created by Google for use on mobile devices, such as smartphones and tablets.*					
Denial of Service	2016-09-11	7.1	OMXCodec.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, 6.x before 2016-09-01, and 7.0 before 2016-09-01 does not validate a certain pointer, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 29421811. **Reference: CVE-2016-3899**	https://android.googlesource.com/platform/frameworks/av/+/97837bb6cbac21ea679843a0037779d3834bed64	O-GOO-ANDRO-210916/261
Denial of Service	2016-09-11	4.3	Telephony in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allows attackers to cause a denial of service (loss of locked-screen 911 TTY functionality) via a crafted application that modifies the TTY mode by broadcasting an intent, aka internal bug 29832693. **Reference: CVE-2016-3898**	https://android.googlesource.com/platform/packages/services/Telephony/+/d1d248d10cf03498efb7041f1a8c9c467482a19d	O-GOO-ANDRO-210916/262
Gain	2016-09-	4.3	The WifiEnterpriseConfig	http://sour	O-GOO-

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

Information	11		class in net/wifi/WifiEnterpriseConfig.java in Wi-Fi 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 2016-09-01 includes a password in the return value of a toString method call, which allows attackers to obtain sensitive information via a crafted application, aka internal bug 25624963. **Reference: CVE-2016-3897**	ce.android.com/security/bulletin/2016-09-01.html	ANDRO-210916/263
Gain Information	2016-09-11	4.3	AOSP Mail 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 2016-09-01 allows attackers to obtain sensitive EmailAccountCacheProvider information via a crafted application, aka internal bug 29767043. **Reference: CVE-2016-3896**	https://android.googlesource.com/platform/packages/apps/Email/+/cb2dfe43f25cb0c32cc73aa4569c0a5186a4ef43	O-GOO-ANDRO-210916/264
Overflow Gain Info	2016-09-11	4.3	Integer overflow in the Region::unflatten function in libs/ui/Region.cpp in mediaserver in Android 6.x before 2016-09-01 and 7.0 before 2016-09-01 allows attackers to obtain sensitive information via a crafted application, aka internal bug 29983260. **Reference: CVE-2016-3895**	https://android.googlesource.com/platform/frameworks/native/+/363247929c35104b3e5ee9e637e9dcf579080aee	O-GOO-ANDRO-210916/265
Gain Information	2016-09-11	4.3	The Qualcomm DMA component in Android before 2016-09-05 on	http://source.android.com/secu	O-GOO-ANDRO-210916/26

			Nexus 6 devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 29618014 and Qualcomm internal bug CR1042033. **Reference: CVE-2016-3894**	rity/bulletin/2016-09-01.html	6
Gain Information	2016-09-11	4.3	The wcdcal_hwdep_ioctl_shared function in sound/soc/codecs/wcdcal-hwdep.c in the Qualcomm sound codec in Android before 2016-09-05 on Nexus 6P devices does not properly copy firmware data, which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 29512527 and Qualcomm internal bug CR856400. **Reference: CVE-2016-3893**	https://source.codeaurora.org/quic/la/kernel/msm-3.10/commit/?id=a7a6ddc91cce7ad5ad55c9709b24bfc80f5ac873	O-GOO-ANDRO-210916/267
Gain Information	2016-09-11	4.3	The Qualcomm SPMI driver in Android before 2016-09-05 on Nexus 5, 5X, 6, and 6P devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28760543 and Qualcomm internal bug CR1024197. **Reference: CVE-2016-3892**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/268
Gain Privileges	2016-09-11	7.6	The Java Debug Wire Protocol (JDWP) implementation in adb/sockets.cpp in Android 4.x before 4.4.4,	http://source.android.com/security/bulletin/2016-	O-GOO-ANDRO-210916/269

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

			5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-09-01 mishandles socket close operations, which allows attackers to gain privileges via a crafted application, aka internal bug 28347842. **Reference: CVE-2016-3890**	09-01.html	
Bypass	2016-09-11	7.2	Android 6.x before 2016-09-01 and 7.0 before 2016-09-01 allows physically proximate attackers to bypass the Factory Reset Protection protection mechanism by accessing (1) an external tile from a system application, (2) the help feature, or (3) the Settings application during a pre-setup stage, aka internal bug 29194585. **Reference: CVE-2016-3889**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/270
Bypass	2016-09-11	2.1	internal/telephony/SMSDispatcher.java in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allows physically proximate attackers to bypass the Factory Reset Protection protection mechanism, and send premium SMS messages during the Setup Wizard provisioning stage, via unspecified vectors, aka internal bug 29420123.	https://android.googlesource.com/platform/frameworks/opt/telephony/+/b8d1aee993dcc565e6576b2f2439a8f5a507cff6	O-GOO-ANDRO-210916/271

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

			Reference: CVE-2016-3888		
Bypass	2016-09-11	6.8	providers/settings/SettingsProvider.java in Android 7.0 before 2016-09-01 does not properly enforce the DISALLOW_CONFIG_VPN setting, which allows attackers to bypass an intended always-on VPN state via a crafted application, aka internal bug 29899712. **Reference: CVE-2016-3887**	https://android.googlesource.com/platform/frameworks/base/+/335702d106797bce8a88044783fa1fc1d5f751d0	O-GOO-ANDRO-210916/272
Gain Privileges	2016-09-11	7.2	systemui/statusbar/phone/QuickStatusBarHeader.java in the System UI Tuner in Android 7.0 before 2016-09-01 does not prevent tuner changes on the lockscreen, which allows physically proximate attackers to gain privileges by modifying a setting, aka internal bug 30107438. **Reference: CVE-2016-3886**	https://android.googlesource.com/platform/frameworks/base/+/6ca6cd5a50311d58a1b7bf8fbef3f9aa29eadcd5	O-GOO-ANDRO-210916/273
Gain Privileges	2016-09-11	9.3	debuggerd/debuggerd.cpp in Debuggerd in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 mishandles the interaction between PTRACE_ATTACH operations and thread exits, which allows attackers to gain privileges via a crafted application, aka internal	https://android.googlesource.com/platform/system/core/+/d7603583f90c2bc6074a4ee2886bd28082d7c65b	O-GOO-ANDRO-210916/274

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

			bug 29555636. **Reference: CVE-2016-3885**		
Bypass	2016-09-11	4.3	server/notification/NotificationManagerService.java in the Notification Manager Service in Android 6.x before 2016-09-01 and 7.0 before 2016-09-01 lacks uid checks, which allows attackers to bypass intended restrictions on method calls via a crafted application, aka internal bug 29421441. **Reference: CVE-2016-3884**	https://android.googlesource.com/platform/frameworks/base/+/61e9103b5725965568e46657f4781dd8f2e5b623	O-GOO-ANDRO-210916/275
NA	2016-09-11	4.3	internal/telephony/SMSDispatcher.java in Telephony in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 does not properly construct warnings about premium SMS messages, which allows attackers to spoof the premium-payment confirmation dialog via a crafted application, aka internal bug 28557603. **Reference: CVE-2016-3883**	https://android.googlesource.com/platform/frameworks/opt/telephony/+/b2c89e6f8962dc7aff88cb38aa3ee67d751edda9	O-GOO-ANDRO-210916/276
Denial of Service; Overflow	2016-09-11	7.1	The decoder_peek_si_internal function in vp9/vp9_dx_iface.c in libvpx in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before	https://android.googlesource.com/platform/external/libvpx/+/4974dcbd0289a2	O-GOO-ANDRO-210916/277

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

			2016-09-01, and 7.0 before 2016-09-01 allows remote attackers to cause a denial of service (buffer over-read, and device hang or reboot) via a crafted media file, aka internal bug 30013856. **Reference: CVE-2016-3881**	530df2ee2a25b5f92775df80da	
Denial of Service; Overflow	2016-09-11	7.1	Multiple buffer overflows in rtsp/ASessionDescription.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, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allow remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 25747670. **Reference: CVE-2016-3880**	https://android.googlesource.com/platform/frameworks/av/+/68f67ef6cf1f41e77337be3bc4bff91f3a3c6324	O-GOO-ANDRO-210916/278
Denial of Service	2016-09-11	7.1	arm-wt-22k/lib_src/eas_mdls.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 2016-09-01 allows remote attackers to cause a denial of service (NULL pointer dereference, and device hang or reboot) via a crafted media file, aka internal bug 29770686. **Reference: CVE-2016-3879**	https://android.googlesource.com/platform/external/sonivox/+/cadfb7a3c96d4fef06656cf37143e1b3e62cae86	O-GOO-ANDRO-210916/279
Denial of Service	2016-09-11	7.1	decoder/ih264d_api.c in mediaserver in Android	https://android.goog	O-GOO-ANDRO-

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

			6.x before 2016-09-01 mishandles the case of decoding zero MBs, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 29493002. **Reference: CVE-2016-3878**	lesource.com/platform/external/libavc/+/7109ce3f8f90a28ca9f0ee6e14f6ac5e414c62cf	210916/280
NA	2016-09-11	10	Unspecified vulnerability in Android before 2016-09-01 has unknown impact and attack vectors. **Reference: CVE-2016-3877**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/281
Bypass	2016-09-11	7.2	providers/settings/SettingsProvider.java in Android 6.x before 2016-09-01 and 7.0 before 2016-09-01 allows physically proximate attackers to bypass the SAFE_BOOT_DISALLOWED protection mechanism and boot to safe mode via the Android Debug Bridge (adb) tool, aka internal bug 29900345. **Reference: CVE-2016-3876**	https://android.googlesource.com/platform/frameworks/base/+/91fc934bb2e5ea59929bb2f574de6db9b5100745	O-GOO-ANDRO-210916/282
Bypass	2016-09-11	7.2	server/wm/WindowManagerService.java in Android 6.x before 2016-09-01 does not enforce the DISALLOW_SAFE_BOOT setting, which allows physically proximate attackers to bypass intended access restrictions and boot to safe mode via unspecified	https://android.googlesource.com/platform/frameworks/base/+/69729fa8b13cadbf3173fe1f389fe4f3b7bd0f9c	O-GOO-ANDRO-210916/283

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

			vectors, aka internal bug 26251884. **Reference: CVE-2016-3875**		
Gain Privileges	2016-09-11	9.3	CORE/HDD/src/wlan_hdd_wext.c in the Qualcomm Wi-Fi driver in Android before 2016-09-05 on Nexus 5X devices does not properly validate the arguments array, which allows attackers to gain privileges via a crafted application that sends a WE_UNIT_TEST_CMD command, aka Android internal bug 29944562 and Qualcomm internal bug CR997797. **Reference: CVE-2016-3874**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/284
Gain Privileges	2016-09-11	9.3	The NVIDIA kernel in Android before 2016-09-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 29518457. **Reference: CVE-2016-3873**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/285
Overflow; Gain Privileges	2016-09-11	9.3	Buffer overflow in 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, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allows attackers to gain privileges via a crafted application, aka internal bug 29421675. **Reference: CVE-2016-3872**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/286

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

Overflow; Gain Privileges	2016-09-11	9.3	Multiple buffer overflows in codecs/mp3dec/SoftMP3.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, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allow attackers to gain privileges via a crafted application, aka internal bug 29422022. **Reference: CVE-2016-3871**	https://android.googlesource.com/platform/frameworks/av/+/c2639afac631f5c1ffddf70ee8a6fe943d0bedf9	O-GOO-ANDRO-210916/287
Gain Privileges	2016-09-11	9.3	omx/SimpleSoftOMXComponent.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, 6.x before 2016-09-01, and 7.0 before 2016-09-01 does not prevent input-port changes, which allows attackers to gain privileges via a crafted application, aka internal bug 29421804. **Reference: CVE-2016-3870**	https://android.googlesource.com/platform/frameworks/av/+/1e9801783770917728b7edbdeff3d0ec09c621ac	O-GOO-ANDRO-210916/288
Gain Privileges	2016-09-11	9.3	The Broadcom Wi-Fi driver in Android before 2016-09-05 on Nexus 5, Nexus 6, Nexus 6P, Nexus 9, Nexus Player, and Pixel C devices allows attackers to gain privileges via a crafted application, aka Android internal bug 29009982 and Broadcom internal bug RB#96070. **Reference: CVE-2016-3869**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/289
Gain	2016-09-	9.3	The Qualcomm power	http://sour	O-GOO-

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

Privileges	11		driver in Android before 2016-09-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28967028 and Qualcomm internal bug CR1032875. **Reference: CVE-2016-3868**	ce.android.com/security/bulletin/2016-09-01.html	ANDRO-210916/290
Gain Privileges	2016-09-11	9.3	The Qualcomm IPA driver in Android before 2016-09-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28919863 and Qualcomm internal bug CR1037897. **Reference: CVE-2016-3867**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/291
Gain Privileges	2016-09-11	9.3	The Qualcomm sound driver in Android before 2016-09-05 on Nexus 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28868303 and Qualcomm internal bug CR1032820. **Reference: CVE-2016-3866**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/292
Gain Privileges	2016-09-11	9.3	The Synaptics touchscreen driver in Android before 2016-09-05 on Nexus 5X and 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 28799389. **Reference: CVE-2016-3865**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/293

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

Gain Privileges	2016-09-11	9.3	The Qualcomm radio interface layer in Android before 2016-09-05 on Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28823714 and Qualcomm internal bug CR913117. **Reference: CVE-2016-3864**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/294
Execute Code; Overflow	2016-09-11	6.8	Multiple stack-based buffer overflows in the AVCC reassembly implementation in Utils.cpp in libstagefright in MediaMuxer in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allow remote attackers to execute arbitrary code via a crafted media file, aka internal bug 29161888. **Reference: CVE-2016-3863**	https://android.googlesource.com/platform/frameworks/av/+/119a012b2a9a186655da4bef3ed4ed8dd9b94c26	O-GOO-ANDRO-210916/295
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09-11	9.3	media/ExifInterface.java 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 2016-09-01 does not properly interact with the use of static variables in libjhead_jni, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a	https://android.googlesource.com/platform/frameworks/base/+/e739d9ca5469ed30129d0fa228e3d0f2878671ac	O-GOO-ANDRO-210916/296

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

			crafted media file, aka internal bug 29270469. **Reference: CVE-2016-3862**		
Denial of Service; Execute Code; Overflow	2016-09-11	9.3	LibUtils in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 mishandles conversions between Unicode character encodings with different encoding widths, which allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow) via a crafted file, aka internal bug 29250543. **Reference: CVE-2016-3861**	https://android.googlesource.com/platform/system/core/+/ecf5fd58a8f50362ce9e8d4245a33d56f29f142b	O-GOO-ANDRO-210916/297
Gain Privileges	2016-09-11	9.3	The Qualcomm camera driver in Android before 2016-09-05 on Nexus 5, 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28815326 and Qualcomm internal bug CR1034641. **Reference: CVE-2016-3859**	http://source.android.com/security/bulletin/2016-09-01.html	O-GOO-ANDRO-210916/298
Overflow; Gain Privileges	2016-09-11	9.3	Buffer overflow in drivers/soc/qcom/subsystem_restart.c in the Qualcomm subsystem driver in Android before 2016-09-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted	https://source.codeaurora.org/quic/la/kernel/msm-3.10/commit/?id=0c148b9a9028c	O-GOO-ANDRO-210916/299

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

			application that provides a long string, aka Android internal bug 28675151 and Qualcomm internal bug CR1022641. **Reference: CVE-2016-3858**	566eac680f19e5d664b483cdee3	
HP					
Integrated Lights-out 3 Firmware: *iLO facilitates remote management of server.*					
Gain Information	2016-09-08	4.3	The TLS implementation in HPE Integrated Lights-Out 3 (aka iLO3) firmware before 1.88 does not properly use a MAC protection mechanism in conjunction with CBC padding, which allows remote attackers to obtain sensitive information via a padding-oracle attack, aka a Vaudenay attack. **Reference: CVE-2016-4379**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05249760	O-HP-INTEG-210916/300
Integrated Lights-out 3 Firmware; Integrated Lights-out 4 Firmware; Integrated Lights-out 4 Mrca Firmware *iLO facilitates remote management of server.*					
Denial of Service; Gain Information	2016-09-08	7.5	Multiple unspecified vulnerabilities in HPE Integrated Lights-Out 3 (aka iLO 3) firmware before 1.88, Integrated Lights-Out 4 (aka iLO 4) firmware before 2.44, and Integrated Lights-Out 4 (aka iLO 4) mRCA firmware before 2.32 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via unknown vectors.	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05236950	O-HP-INTEG-210916/301

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

			Reference: CVE-2016-4375		
Huawei					
Ch121 V3 Server Firmware;Ch140 V3 Server Firmware;Ch220 V3 Server Firmware;Ch222 V3 Server Firmware;Ch226 V3 Server Firmware;Rh1288 V3 Server Firmware;Rh2288 V3 Server Firmware;X6800 V3 Server Firmware;Xh620 V3 Server Firmware *The HUAWEI RH series is a new-generation 1U dual-socket rack server; Huawei Fusion Server XH Server series is a full-height dual-socket server node.*					
Gain Information	2016-09-07	4.3	Huawei X6800 and XH620 V3 servers with software before V100R003C00SPC606, RH1288 V3 servers with software before V100R003C00SPC613, RH2288 V3 servers with software before V100R003C00SPC617, CH140 V3 and CH226 V3 servers with software before V100R001C00SPC122, CH220 V3 servers with software before V100R001C00SPC201, and CH121 V3 and CH222 V3 servers with software before V100R001C00SPC202 might allow remote attackers to decrypt encrypted data and consequently obtain sensitive information by leveraging selection of an insecure SSH encryption algorithm. **Reference: CVE-2016-6838**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160817-02-server-en	O-HUA-CH121-210916/302
Honor 4c Firmware *Huawei Honor 4C smartphone was launched in April 2015.The Huawei Honor 4C is a dual SIM (GSM and GSM) smartphone that accepts two Micro-SIM.*					

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

Denial of Service ; Gain Privileges	2016-09-07	6.9	The Camera driver in Huawei Honor 4C smartphones with software CHM-UL00C00 before CHM-UL00C00B564, CHM-TL00C01 before CHM-TL00C01B564, and CHM-TL00C00 before CHM-TL00HC00B564 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6180, CVE-2016-6181, CVE-2016-6182, and CVE-2016-6183. **Reference: CVE-2016-6184**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160716-01-smartphone-en	O-HUA-HONOR-210916/303
Denial of Service ; Gain Privileges	2016-09-07	6.9	The Camera driver in Huawei Honor 4C smartphones with software CHM-UL00C00 before CHM-UL00C00B564, CHM-TL00C01 before CHM-TL00C01B564, and CHM-TL00C00 before CHM-TL00HC00B564 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6180, CVE-2016-6181, CVE-2016-6182, and CVE-2016-6184. **Reference: CVE-2016-6183**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160716-01-smartphone-en	O-HUA-HONOR-210916/304
Denial of Service ;	2016-09-07	9.3	The Camera driver in Huawei Honor 4C	http://www.huawei.co	O-HUA-HONOR-

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

Gain Privileges			smartphones with software CHM-UL00C00 before CHM-UL00C00B564, CHM-TL00C01 before CHM-TL00C01B564, and CHM-TL00C00 before CHM-TL00HC00B564 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6180, CVE-2016-6181, CVE-2016-6183, and CVE-2016-6184. **Reference: CVE-2016-6182**	m/en/psirt/security-advisories/huawei-sa-20160716-01-smartphone-en	210916/305
Denial of Service ; Gain Privileges	2016-09-07	6.9	The Camera driver in Huawei Honor 4C smartphones with software CHM-UL00C00 before CHM-UL00C00B564, CHM-TL00C01 before CHM-TL00C01B564, and CHM-TL00C00 before CHM-TL00HC00B564 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6180, CVE-2016-6182, CVE-2016-6183, and CVE-2016-6184. **Reference: CVE-2016-6181**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160716-01-smartphone-en	O-HUA-HONOR-210916/306
Denial of Service ; Gain Privileges	2016-09-07	6.9	The Camera driver in Huawei Honor 4C smartphones with software CHM-UL00C00	http://www.huawei.com/en/psirt/security-	O-HUA-HONOR-210916/307

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

			before CHM-UL00C00B564, CHM-TL00C01 before CHM-TL00C01B564, and CHM-TL00C00 before CHM-TL00HC00B564 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6181, CVE-2016-6182, CVE-2016-6183, and CVE-2016-6184. **Reference: CVE-2016-6180**	advisories/huawei-sa-20160716-01-smartphone-en	
Denial of Service ; Gain Privileges	2016-09-07	6.9	The WiFi driver in Huawei Honor 6 smartphones with software H60-L01 before H60-L01C00B850, H60-L11 before H60-L11C00B850, H60-L21 before H60-L21C00B850, H60-L02 before H60-L02C00B850, H60-L12 before H60-L12C00B850, and H60-L03 before H60-L03C01B850 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application. **Reference: CVE-2016-6179**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160713-01-smartphone-en	O-HUA-HONOR-210916/308
Rh1288 V3 Server Firmware;Rh2288 V3 Server Firmware; Rh2288h V3 Server Firmware;Rh5885 V3 Server Firmware;Xh620 V3 Server Firmware; Xh622 V3 Server Firmware;Xh628 V3 Server Firmware *The HUAWEI RH series is a new-generation 1U dual-socket rack server; Huawei FusionServer XH Server series is a full-height dual-socket server node.*					
Denial of Service	2016-09-07	2.1	The Intelligent Baseboard Management Controller (iBMC) in Huawei RH1288 V3 servers with software	http://www.huawei.com/en/psirt/security-	O-HUA-RH128-210916/309

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

			before V100R003C00SPC613; RH2288 V3 servers with software before V100R003C00SPC617; RH2288H V3 servers with software before V100R003C00SPC515; RH5885 V3 servers with software before V100R003C10SPC102; and XH620 V3, XH622 V3, and XH628 V3 servers with software before V100R003C00SPC610 allows local users to cause a denial of service (iBMC resource consumption) via unspecified vectors. **Reference: CVE-2016-6900**	advisories/huawei-sa-20160824-01-server-en	
Gain Information	2016-09-07	4.3	The Intelligent Baseboard Management Controller (iBMC) in Huawei RH1288 V3 servers with software before V100R003C00SPC613, RH2288 V3 servers with software before V100R003C00SPC617, RH2288H V3 servers with software before V100R003C00SPC515, RH5885 V3 servers with software before V100R003C10SPC102, and XH620 V3, XH622 V3, and XH628 V3 servers with software before V100R003C00SPC610 might allow remote attackers to decrypt encrypted data and consequently obtain	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160824-02-server-en	O-HUA-RH128-210916/310

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

			sensitive information by leveraging selection of an insecure SSL encryption algorithm. **Reference: CVE-2016-6899**		
NA	2016-09-07	5	Huawei XH620 V3, XH622 V3, and XH628 V3 servers with software before V100R003C00SPC610, RH1288 V3 servers with software before V100R003C00SPC613, RH2288 V3 servers with software before V100R003C00SPC617, and RH2288H V3 servers with software before V100R003C00SPC515 allow remote attackers to obtain passwords via a brute-force attack, related to "lack of authentication protection mechanisms." **Reference: CVE-2016-6825**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160817-01-server-en	O-HUA-RH128-210916/311
S7700 Firmware;S9300 Firmware;S9700 Firmware/S12700 *Huawei S7700 Series Smart Routing Switches for campus networks; The S9300 is a carrier-class chassis switch with six service slots. It is highly redundant to meet carrier class requirements for high availability.*					
Gain Information	2016-09-07	5	Huawei S7700, S9300, S9700, and S12700 devices with software before V200R008C00SPC500 use random numbers with insufficient entropy to generate self-signed certificates, which makes it easier for remote attackers to discover private keys by leveraging knowledge of a certificate.	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160810-01-certificate-en	O-HUA-S7700-210916/312

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

			Reference: CVE-2016-6670		
IBM					
Mq Appliance Firmware *IBM MQ Appliance provides the application connectivity performance of IBM MQ software in a physical messaging appliance.*					
Execute Code	2016-09-02	4.6	MQCLI on IBM MQ Appliance M2000 and M2001 devices allows local users to execute arbitrary shell commands via a crafted (1) Disaster Recovery or (2) High Availability command. **Reference: CVE-2016-5879**	http://www-01.ibm.com/support/docview.wss?uid=swg21987697	O-IBM-MQAP-210916/313
Juniper					
Junos *Junos OS is the FreeBSD-based operating system used in Juniper Networks hardware routers. It is an operating system that is used in Juniper's routing, switching and security devices.*					
Bypass	2016-09-09	6.4	PKId in Juniper Junos OS before 12.1X44-D52, 12.1X46 before 12.1X46-D37, 12.1X47 before 12.1X47-D30, 12.3 before 12.3R12, 12.3X48 before 12.3X48-D20, 13.3 before 13.3R10, 14.1 before 14.1R8, 14.1X53 before 14.1X53-D40, 14.2 before 14.2R7, 15.1 before 15.1R4, 15.1X49 before 15.1X49-D20, 15.1X53 before 15.1X53-D60, and 16.1 before 16.1R1 allow remote attackers to bypass an intended certificate validation mechanism via a self-signed certificate with an Issuer name that matches a valid CA certificate enrolled in Junos.	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10755	O-JUN-JUNOS-210916/314

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

			Reference: CVE-2016-1280		
Gain Privileges Gain Information	2016-09-09	10	J-Web in Juniper Junos OS before 12.1X46-D45, 12.1X46-D50, 12.1X47 before 12.1X47-D35, 12.3 before 12.3R12, 12.3X48 before 12.3X48-D25, 13.3 before 13.3R10, 13.3R9 before 13.3R9-S1, 14.1 before 14.1R7, 14.1X53 before 14.1X53-D35, 14.2 before 14.2R6, 15.1 before 15.1A2 or 15.1F4, 15.1X49 before 15.1X49-D30, and 15.1R before 15.1R3 might allow remote attackers to obtain sensitive information and consequently gain administrative privileges via unspecified vectors. **Reference: CVE-2016-1279**	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10754	O-JUN-JUNOS-210916/315
Denial of Service	2016-09-09	7.1	Juniper Junos OS before 12.1X46-D50, 12.1X47 before 12.1X47-D40, 12.3X48 before 12.3X48-D30, 13.3 before 13.3R9, 14.1 before 14.1R8, 14.1X53 before 14.1X53-D40, 14.2 before 14.2R6, 15.1 before 15.1F6 or 15.1R3, and 15.1X49 before 15.1X49-D40, when configured with a GRE or IPIP tunnel, allow remote attackers to cause a denial of service (kernel panic) via a crafted ICMP packet. **Reference: CVE-2016-1277**	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10752	O-JUN-JUNOS-210916/316

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

Gain Information	2016-09-09	6.1	Juniper Junos OS before 13.3R9, 14.1R6 before 14.1R6-S1, and 14.1 before 14.1R7, when configured with VPLS routing-instances, allows remote attackers to obtain sensitive mbuf information by injecting a flood of Ethernet frames with IPv6 MAC addresses directly into a connected interface. **Reference: CVE-2016-1275**	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10750	O-JUN-JUNOS-210916/317
Denial of Service	2016-09-09	7.8	Juniper Junos OS before 12.1X46-D45, 12.1X46-D50, 12.1X47 before 12.1X47-D35, 12.3X48 before 12.3X48-D30, 13.3 before 13.3R9-S1, 14.1 before 14.1R7, 14.2 before 14.2R6, 15.1 before 15.1F2-S5, 15.1F4 before 15.1F4-S2, 15.1R before 15.1R2-S3, 15.1 before 15.1R3, and 15.1X49 before 15.1X49-D40 allow remote attackers to cause a denial of service (kernel crash) via a crafted UDP packet destined to the interface IP address of a 64-bit OS device. **Reference: CVE-2016-1263**	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10758	O-JUN-JUNOS-210916/318
Linux					
Linux Kernel *The Linux kernel is a Unix-like computer operating system kernel. The Linux operating system is based on it and deployed on both traditional computer systems such as personal computers and servers, usually in the form of Linux distributions*					
Denial of Service;	2016-08-30	10	Multiple integer overflows in the MDSS driver for the	https://www.codeaur	O-LIN-LINUX-

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

Overflow			Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service or possibly have unspecified other impact via a large size value, related to mdss_compat_utils.c, mdss_fb.c, and mdss_rotator.c. **Reference: CVE-2016-5344**	ora.org/integer-overflow-mdss-driver-cve-2016-5344	210916/319
Denial of Service; Overflow	2016-08-30	7.2	Heap-based buffer overflow in the wcnss_wlan_write function in drivers/net/wireless/wcnss/wcnss_wlan.c in the wcnss_wlan device driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service or possibly have unspecified other impact by writing to /dev/wcnss_wlan with an unexpected amount of data. **Reference: CVE-2016-5342**	https://www.codeaurora.org/buffer-overflow-vulnerability-wcnsswlan-write-cve-2016-5342	O-LIN-LINUX-210916/320
Microsoft					
Windows 10 *Windows 10 is a personal computer operating system developed and released by Microsoft as part of the Windows NT family of operating systems.*					
Denial of Service	2016-09-14	7.8	Microsoft Windows 10 Gold and 1511 allows	http://technet.micros	O-MIC-WINDO-

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

Overflow			attackers to cause a denial of service via unspecified vectors, aka "Windows Denial of Service Vulnerability." **Reference: CVE-2016-3369**	oft.com/en-us/security/bulletin/ms16-110	210916/321
Execute Code; Overflow	2016-09-14	9.3	The Graphics Device Interface (GDI) in Microsoft Windows 10 1607 allows remote attackers to execute arbitrary code via a crafted document, aka "GDI Remote Code Execution Vulnerability." **Reference: CVE-2016-3356**	http://technet.microsoft.com/en-us/security/bulletin/ms16-106	O-MIC-WINDO-210916/322
NA	2016-09-14	7.2	Microsoft Windows 10 Gold, 1511, and 1607 does not properly enforce permissions, which allows local users to obtain Administrator access via a crafted DLL, aka "Windows Permissions Enforcement Elevation of Privilege Vulnerability." **Reference: CVE-2016-3346**	http://technet.microsoft.com/en-us/security/bulletin/ms16-110	O-MIC-WINDO-210916/323
Gain Information	2016-09-14	2.1	The Secure Kernel Mode feature in Microsoft Windows 10 Gold and 1511 allows local users to obtain sensitive information via a crafted application, aka "Windows Secure Kernel Mode Information Disclosure Vulnerability." **Reference: CVE-2016-3344**	http://technet.microsoft.com/en-us/security/bulletin/ms16-113	O-MIC-WINDO-210916/324

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

Windows 10;Windows 7;Windows 8.1;Windows Rt 8.1;Windows Server 2008;Windows Server 2012;Windows Vista *Windows is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems. Windows Server series is Microsoft Windows server line of operating systems.*					
Gain Information	2016-09-14	4.3	The kernel API 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, 1511, and 1607 does not properly implement registry access control, which allows local users to obtain sensitive account information via a crafted application, aka "Windows Kernel Elevation of Privilege Vulnerability." **Reference: CVE-2016-3373**	http://technet.microsoft.com/en-us/security/bulletin/ms16-111	O-MIC-WINDO-210916/325
Gain Information	2016-09-14	4.3	The kernel API 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, 1511, and 1607 does not properly enforce permissions, which allows local users to obtain sensitive information via a crafted application, aka "Windows Kernel Elevation of Privilege Vulnerability." **Reference: CVE-2016-3371**	http://technet.microsoft.com/en-us/security/bulletin/ms16-111	O-MIC-WINDO-210916/326

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

Execute Code; Overflow	2016-09-14	9	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, 1511, and 1607 allow remote authenticated users to execute arbitrary code by leveraging a domain account to make a crafted request, aka "Windows Remote Code Execution Vulnerability." **Reference: CVE-2016-3368**	http://technet.microsoft.com/en-us/security/bulletin/ms16-110	O-MIC-WINDO-210916/327
Gain Privileges	2016-09-14	7.2	The Graphics Device Interface (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, 1511, and 1607 allows local users to gain privileges via a crafted application, aka "GDI Elevation of Privilege Vulnerability." **Reference: CVE-2016-3355**	http://technet.microsoft.com/en-us/security/bulletin/ms16-106	O-MIC-WINDO-210916/328
Bypass	2016-09-14	4.3	The Graphics Device Interface (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	http://technet.microsoft.com/en-us/security/bulletin/ms16-106	O-MIC-WINDO-210916/329

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

			Gold, 1511, and 1607 allows local users to bypass the ASLR protection mechanism via a crafted application, aka "GDI Information Disclosure Vulnerability." **Reference: CVE-2016-3354**		
Gain Privileges	2016-09-14	9.3	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, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." **Reference: CVE-2016-3348**	http://technet.microsoft.com/en-us/security/bulletin/ms16-106	O-MIC-WINDO-210916/330
Execute Code	2016-09-14	9	The SMBv1 server 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, 1511, and 1607 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Authenticated Remote Code Execution Vulnerability." **Reference: CVE-2016-3345**	http://technet.microsoft.com/en-us/security/bulletin/ms16-114	O-MIC-WINDO-210916/331
Gain	2016-09-	4.6	The kernel in Microsoft	http://tech	O-MIC-

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

Privileges	14		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, 1511, and 1607 mishandles session objects, which allows local users to hijack sessions, and consequently gain privileges, via a crafted application, aka "Windows Session Object Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3305. **Reference: CVE-2016-3306**	net.microsoft.com/en-us/security/bulletin/ms16-111	WINDO-210916/332
Gain Privileges	2016-09-14	4.6	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, 1511, and 1607 mishandles session objects, which allows local users to hijack sessions, and consequently gain privileges, via a crafted application, aka "Windows Session Object Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3306. **Reference: CVE-2016-3305**	http://technet.microsoft.com/en-us/security/bulletin/ms16-111	O-MIC-WINDO-210916/333
NA	2016-09-14	4.3	Microsoft Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511,	http://technet.microsoft.com/en	O-MIC-WINDO-210916/33

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

			and 1607 do not properly check NTLM SSO requests for MSA logins, which makes it easier for remote attackers to determine passwords via a brute-force attack on NTLM password hashes, aka "Microsoft Information Disclosure Vulnerability." **Reference: CVE-2016-3352**	-us/security/bulletin/ms16-110	4
Windows 10;Windows 8.1;Windows Rt 8.1;Windows Server 2012 *Windows is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems. Windows Server series is Microsoft Windows server line of operating systems.*					
Gain Privileges	2016-09-14	7.2	The kernel-mode drivers in Microsoft 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." **Reference: CVE-2016-3349**	http://technet.microsoft.com/en-us/security/bulletin/ms16-106	O-MIC-WINDO-210916/335
Execute Code	2016-09-14	6.2	Microsoft Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607, when the lock screen is enabled, do not properly restrict the loading of web content, which allows physically proximate attackers to execute arbitrary code via a (1) crafted Wi-Fi access point or (2) crafted mobile-broadband device, aka "Windows Lock Screen Elevation of	http://technet.microsoft.com/en-us/security/bulletin/ms16-112	O-MIC-WINDO-210916/336

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

			Privilege Vulnerability." **Reference: CVE-2016-3302**		
Windows Server 2008;Windows Vista *Windows is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems.Windows Server series is Microsoft Windows server line of operating systems.*					
Denial of Service	2016-09-14	3.6	The kernel API in Microsoft Windows Vista SP2 and Windows Server 2008 SP2 does not properly enforce permissions, which allows local users to spoof processes, spoof inter-process communication, or cause a denial of service via a crafted application, aka "Windows Kernel Elevation of Privilege Vulnerability." **Reference: CVE-2016-3372**	http://technet.microsoft.com/en-us/security/bulletin/ms16-111	O-MIC-WINDO-210916/337
Moxa					
Oncell G3001 Firmware; Oncell G3100v2 Firmware:NA					
Gain Information	2016-08-23	2.1	Moxa OnCell G3100V2 devices before 2.8 and G3111, G3151, G3211, and G3251 devices before 1.7 use cleartext password storage, which makes it easier for local users to obtain sensitive information by reading a configuration file. **Reference: CVE-2016-5812**	https://ics-cert.us-cert.gov/advisories/ICSA-16-236-01	O-MOX-ONCEL-210916/338
NA	2016-08-23	10	Moxa OnCell G3100V2 devices before 2.8 and G3111, G3151, G3211, and G3251 devices before 1.7 do not properly restrict authentication attempts, which makes it easier for remote	https://ics-cert.us-cert.gov/advisories/ICSA-16-236-01	O-MOX-ONCEL-210916/339

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

			attackers to obtain access via a brute-force attack. **Reference: CVE-2016-5799**		
Nuuo					
Nvrmini 2;Nvrsolo *NUUO NVRmini 2 is the lightweight, portable NVR solution with NAS functionality; NVRsolo is NUUO's answer to hassle free, lightweight NVR system.*					
NA	2016-08-31	10	NUUO NVRmini 2 1.0.0 through 3.0.0 and NUUO NVRsolo 1.0.0 through 3.0.0 have hardcoded root credentials, which allows remote attackers to obtain administrative access via unspecified vectors. **Reference: CVE-2016-5678**	http://www.kb.cert.org/vuls/id/856152	O-NUU-NVRMI-210916/340
Vmware					
Photon OS *Photon OS is a minimal Linux container host, optimized to run on VMware platforms.*					
NA	2016-08-30	9.3	VMware Photos OS OVA 1.0 before 2016-08-14 has a default SSH public key in an authorized_keys file, which allows remote attackers to obtain SSH access by leveraging knowledge of the private key. **Reference: CVE-2016-5333**	http://www.vmware.com/security/advisories/VMSA-2016-0012.html	O-VMW-PHOTO-210916/341
Application; Operating System (A/OS)					
Canonical/Qemu					
Ubuntu Linux/Qemu *Ubuntu Linux is an Operating System/ QEMU supports virtualization when executing under the Xen hypervisor or using the KVM kernel module in Linux.*					
Denial of Service	2016-09-02	1.5	The megasas_lookup_frame function in QEMU, when built with MegaRAID SAS	https://bugzilla.redhat.com/show_bug.cg	A-OS-CAN-UBUNT-210916/342

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

			8708EM2 Host Bus Adapter emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds read and crash) via unspecified vectors. **Reference: CVE-2016-5107**	i?id=1336461	
Denial of Service	2016-09-02	1.5	The megasas_dcmd_set_properties function in hw/scsi/megasas.c in QEMU, when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, allows local guest administrators to cause a denial of service (out-of-bounds write access) via vectors involving a MegaRAID Firmware Interface (MFI) command. **Reference: CVE-2016-5106**	https://bugzilla.redhat.com/show_bug.cgi?id=1339578	A-OS-CAN-UBUNT-210916/343
Gain Information	2016-09-02	1.9	The megasas_dcmd_cfg_read function in hw/scsi/megasas.c in QEMU, when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, uses an uninitialized variable, which allows local guest administrators to read host memory via vectors involving a MegaRAID Firmware Interface (MFI) command. **Reference: CVE-2016-5105**	https://bugzilla.redhat.com/show_bug.cgi?id=1339583	A-OS-CAN-UBUNT-210916/344

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

Denial of Service	2016-09-02	1.5	QEMU (aka Quick Emulator), when built with VMWARE PVSCSI paravirtual SCSI bus emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds array access) via vectors related to the (1) PVSCSI_CMD_SETUP_RINGS or (2) PVSCSI_CMD_SETUP_MSG_RING SCSI command. **Reference: CVE-2016-4952**	https://bugzilla.redhat.com/show_bug.cgi?id=1334384	A-OS-CAN-UBUNT-210916/345
Denial of Service; Execute Code	2016-09-07	7.2	The esp_do_dma function in hw/scsi/esp.c in QEMU (aka Quick Emulator), when built with ESP/NCR53C9x controller emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) or execute arbitrary code on the QEMU host via vectors involving DMA read into ESP command buffer. **Reference: CVE-2016-6351**	http://git.qemu.org/?p=qemu.git;a=commit;h=926cde5f3e4d2504ed161ed0cb771ac7cad6fd11	A-OS-CAN-UBUNT-210916/346
Canonical; Fedoraproject; Novell/Gnome					
Ubuntu Linux/Fedora/Leap; Opensuse/Eye Of Gnome *The Linux kernel is a Unix-like computer operating system kernel. The Linux operating system is based on it and deployed on both traditional computer systems such as personal computers and servers, usually in the form of Linux distributions/ Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat. / LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solution; The openSUSE project is a worldwide effort that promotes the use of Linux/ Eye of Genome is the official image viewer for the Gnome desktop environment.*					
Denial of Service	2016-09-07	5	Eye of GNOME (aka eog) 3.16.5, 3.17.x, 3.18.x	https://git.gnome.org	A-OS-CAN-UBUNT-

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

			before 3.18.3, 3.19.x, and 3.20.x before 3.20.4, when used with glib before 2.44.1, allow remote attackers to cause a denial of service (out-of-bounds write and crash) via vectors involving passing invalid UTF-8 to GMarkup. **Reference: CVE-2016-6855**	/browse/eog/plain/NEWS?h=3.20.4	210916/347
Canonical; Novell/GNU					
Ubuntu Linux/Leap; Opensuse/Libidn *Ubuntu is completely free to download, use and share/ LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solution; The openSUSE project is a worldwide effort that promotes the use of Linux/ GNU's Libidn's purpose is to encode and decode internationalized domain names.*					
Denial of Service	2016-09-07	5	The idna_to_ascii_4i function in lib/idna.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via 64 bytes of input. **Reference: CVE-2016-6261**	http://git.savannah.gnu.org/cgit/libidn.git/commit/?id=f20ce1128fb7f4d33297eee307dddaf0f92ac72d	A-OS-CAN-UBUNT-210916/348
Gain Information	2016-09-07	5	idn in libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read, a different vulnerability than CVE-2015-8948. **Reference: CVE-2016-6262**	http://git.savannah.gnu.org/cgit/libidn.git/commit/?id=5e3cb9c7b5bf0ce665b9d68f5ddf095af5c9ba60	A-OS-CAN-UBUNT-210916/349
Gain Information	2016-09-07	5	idn in GNU libidn before 1.33 might allow remote	http://git.savannah.gnu.org/cgit/libidn.git/commit/?	A-OS-CAN-UBUNT-210916/350

			attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read. **Reference: CVE-2015-8948**	id=570e68886c41c2e765e6218cb317d9a9a447a041	
Debian/Drupal					
Debian Linux/Drupal *Debian is an operating system and a distribution of Free Software/ Drupal is a scalable, open platform for web content management and digital experiences. Drupal provides deep capabilities and endless flexibility on the web.*					
Gain Privileges	2016-09-09	6.5	The User module in Drupal 7.x before 7.44 allows remote authenticated users to gain privileges via vectors involving contributed or custom code that triggers a rebuild of the user profile form. **Reference: CVE-2016-6211**	https://www.drupal.org/SA-CORE-2016-002	A-OS-DEB-DEBIA-210916/351
Debian/Rubyonrails					
Debian Linux/Ruby On Rails *Debian Linux is an Operating System/ Ruby on Rails is open source software to building web application.*					
Cross-site scripting	2016-09-07	4.3	Cross-site scripting (XSS) vulnerability in Action View in Ruby on Rails 3.x before 3.2.22.3, 4.x before 4.2.7.1, and 5.x before 5.0.0.1 might allow remote attackers to inject arbitrary web script or HTML via text declared as "HTML safe" and used as attribute values in tag handlers. **Reference: CVE-2016-6316**	http://weblog.rubyonrails.org/2016/8/11/Rails-5-0-0-1-4-2-7-2-and-3-2-22-3-have-been-released/	A-OS-DEB-DEBIA-210916/352
Fedoraproject/Freeipa					

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

Fedora/Freeipa *Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project/ FreeIPA is an integrated Identity and Authentication solution for Linux/UNIX networked environments.*					
NA	2016-09-07	4	The cert_revoke command in FreeIPA does not check for the "revoke certificate" permission, which allows remote authenticated users to revoke arbitrary certificates by leveraging the "retrieve certificate" permission. **Reference: CVE-2016-5404**	https://fedorahosted.org/freeipa/ticket/6232	A-OS-FED-FEDOR-210916/353
Novell/Roundcube					
Leap/Webmail *LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solution/ Webmail is a free and open source webmail solution with a desktop-like user interface which is easy to install/configure and that runs on a standard LAMPP server.*					
Denial of Service; Cross Site Request Forgery	2016-08-25	6.8	Cross-site request forgery (CSRF) vulnerability in Roundcube Webmail before 1.1.5 allows remote attackers to hijack the authentication of users for requests that download attachments and cause a denial of service (disk consumption) via unspecified vectors. **Reference: CVE-2016-4069**	https://github.com/roundcube/roundcubemail/commit/4a408843b0ef816daf70a472a02b78cd6073a4d5	A-OS-NOV-LEAP/-210916/354
Hardware; Operating System (H/OS)					
D-link					
Dir-817l(w) Firmware;Dir-818l(w) Firmware;Dir-823 Firmware;Dir-850l; Firmare;Dir-868l Firmware;Dir-880l Firmware;Dir-885l Firmware;Dir-890l Firmware;Dir-895l Firmware/Dir-822 Firmware *The D-Link Xtreme N Dual Band Gigabit Router (DIR-825) uses dual band technology to support 2.4GHz & 5GHz wireless signals at the same time. This allows you to check e-mail and browse the Internet using the 2.4GHz band while simultaneously streaming High-Definition (HD) movies and other media on the*					

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

5GHz band.					
Execute Code; Overflow	2016-08-25	9.3	Stack-based buffer overflow in dws/api/Login on D-Link DIR-850L B1 2.07 before 2.07WWB05, DIR-817 Ax, DIR-818LW Bx before 2.05b03beta03, DIR-822 C1 3.01 before 3.01WWb02, DIR-823 A1 1.00 before 1.00WWb05, DIR-895L A1 1.11 before 1.11WWb04, DIR-890L A1 1.09 before 1.09b14, DIR-885L A1 1.11 before 1.11WWb07, DIR-880L A1 1.07 before 1.07WWb08, DIR-868L B1 2.03 before 2.03WWb01, and DIR-868L C1 3.00 before 3.00WWb01 devices allows remote attackers to execute arbitrary code via a long session cookie. **Reference: CVE-2016-5681**	http://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10063	H-OS-D-L-DIR-8-210916/355

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