() Joine	National Cri		nformation Infrastructur CVE Report 16 <sup>th</sup> Aug - 15 <sup>th</sup> Sept 2010		n Centre . 03 No. 15
Vulnerabili ty Type(s)	Publish Date	CVS S	Description	Patch	NCIIPC ID
			Application(A)		
Accellion					
access to er	opliance by <i>p</i> iterprise cor	itent s	on is a secure file sharing sources by allowing interna on any type of device from	al and exter	nal users to
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. <b>Reference: CVE-2016-</b> <b>5664</b>	http://www .kb.cert.or g/vuls/id/3 05607	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. <b>Reference: CVE-2016-</b> 5663	http://www .kb.cert.or g/vuls/id/3 05607	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.or g/vuls/id/3 05607	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

			Refer	ence: C	/F-201	6-				
			5662		201					
Adobe	1									
Acrobat; A	crobat Dc; /	Acroba	t Read	er Dc; l	Reader	•				
	to convert,									
	is a trusted l									
	lard for relial									
	ler is the m								ing, ci	reating,
managing a	nd manipulat	Ing PD		Reader		FORM	al)	mes.		
				t before		7				
				t and Ac		<i>'</i> ,				
				DC Clas		ore				
			15.006	.30198,	and					
				t and Ac						
				DC Con						
				15.017.						
				vs and C ers to ex		w				
				ry code		ه م				
				of servic		Cu				
				ry corru	-	/ia				
				ified ve						
				nt vulne	-					
				VE-2016						
				16-4192	•					
				193, CV CVE-201						
				16-4196		,				
				197, CV		-				
				CVE-201						
			CVE-20	16-4200	), CVE-					
				201, CV						
				CVE-201						
				16-4204	•					
				205, CV						
Denial of			-	CVE-201			ht	tps://hel		
Service;				211, CV				.adobe.		
Execute				CVE-201				m/secur	-	
Code;				16-4214				/produc		
Overflow;				250, CV			s/a	acrobat/	A-AI	
Memory	2016-08-		-	CVE-201		,		sb16-		OB-
Corruption	26	10	CVE-20	16-4254	1, CVE-		26	5.html	210	916/04
CV 🖌										
Scoring	0-1 1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10
Scale										

Denial of Service;		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,	https://hel px.adobe.	
		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-		
		CVE-2016-4268, and CVE-2016-4269. <b>Reference: CVE-2016-</b> 4270 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,		

				_							
				Refere	ence: C	VE-201	.6-				
	<u> </u>			Adobe	Reader		7				
					t before t and Ac		Ι,				
					DC Clas		ore				
					.30198, t and Ac						
					DC Cor		5				
					15.017.						
					vs and C ers to ex		ow				
					ry code		e a				
					of servic	-					
				-	ry corru	•					
				differer	nt vulne	rability					
					VE-2016 )16-4192						
					193, CV		-				
					CVE-201						
					16-4190 197, CV	•					
				4198, 0	CVE-201	6-4199	,				
					16-4200 201, CV	•					
					CVE-201						
					16-4204						
					205, CV CVE-201						
				CVE-20	16-4208	B, CVE-					
					211, CV CVE-201						
					16-421		•				
Denial of					250, CV			64	<b>t</b> ion of 1/le = 1		
Denial of Service;				-	CVE-201 16-4254		-		tps://hel adobe.		
Execute				2016-4	265, CV	E-2016	-	co	m/secur		
Code; Overflow;					CVE-201		,	-	/produc acrobat/		-00
Memory	20	16-08-			16-420			ap	sb16-	ACR	OB-
Corruption		26	10	Refere	ence: C	VE-201	.6-	26	5.html	210	916/06
CV	0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10
Scoring Scale											

			4268							
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-26	10	Adobe Acrobat Reader 15.006 Acrobat Reader before Window attacke arbitrar denial o (memo unspec differer than CV CVE-20 2016-4 4194, C CVE-20 2016-4 4198, C CVE-20 2016-4 4202, C CVE-20 2016-4 4202, C CVE-20 2016-4 4206, C CVE-20 2016-4 4212, C CVE-20 2016-4 4251, C CVE-20 2016-4 4251, C CVE-20 2016-4 4251, C CVE-20 2016-4	Reader a before and Ac DC Clas 30198, and Ac DC Con 5.017.2 vs and C rs to exe y code o f servic ry corru ified vec t vulner /E-2016 16-4192 193, CV 205, CV 2	11.0.1 robat sic bef and robat tinuous 20050 ( 20050 (	ore son ow e a /ia -, -, -, -, -, -, -, -, -, -, -, -, -,	px.a com ity/µ s/ac aps	os://hel adobe. n/secur oroduct crobat/ b16- ntml	ACR 2109	-
CV Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9	9-10

			4267		
			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-		
Donial of			4251, CVE-2016-4252,	bttps://bal	
Denial of			CVE-2016-4254, CVE- 2016-4265, CVE-2016-	https://hel	
Service; Execute			,	px.adobe.	
Code;			4267, CVE-2016-4268, CVE-2016-4269, and	com/secur	
Overflow;			CVE-2016-4269, and CVE-2016-4270.	ity/product s/acrobat/	A-ADO-
Memory	2016-08-		Reference: CVE-2016-	apsb16-	A-ADO- ACROB-
Corruption	2010-08-	10	4266	26.html	210916/08
Contraption	20	10	7200	20.11(111	210310/00

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;			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- 4198, CVE-2016-4203, CVE-2016-4204, CVE- 2016-4205, CVE-2016- 4206, CVE-2016-4203, CVE-2016-4204, CVE- 2016-4211, CVE-2016- 4206, CVE-2016-4207, CVE-2016-4214, 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-2016-4269, and CVE-2016-4270.	https://hel px.adobe. com/secur ity/product s/acrobat/	A-ADO-
,	2016-08- 26	10	,		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;         2016-08- 26         10         Adobe Reader and Acrobat before 11.0.16, Reader DC Classic before         px.ad com/ tity/pro- ity/pro- ity/pro- darbat and Acrobat           Overflow; Memory Corruption         15.006.30172, and Acrobat and Acrobat         apsb1           Reader DC Classic before         14.htr           before 15.016.20039 on Windows and OS X allow attackers to execute         apsb1           arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-10337, 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- 2016-1088, CVE- 2016-1088, CVE- 2016-1093, CVE-2016- 1095, CVE-2016-1116, CVE-2016-1118, CVE- 2016-1129, CVE-2016- 1120, CVE-2016-1112, CVE-2016-1123, CVE- 2016-1124, CVE- 2016-1125, CVE-2016- 1130, CVE-2016-1127, CVE-2016-1128, CVE- 2016-1129, CVE-2016- 1130, CVE-2016-00408, CVE-2016-004089, CVE- 2016-04099, CVE-2016- 1130, CVE-2016-00408, CVE-2016-00409, CVE-2016- 1130, CVE-2016-00408, CVE-2016-00409, CVE-2016- 104093, CVE-2016-00408, CVE-2016-00409, CVE-2016- 1030, CVE-2016-00408, CVE-2016-00409, CVE-2016- 104090, CVE	lobe. ACR secur 2109 oduct obat/ 16-	
CV         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7           Scale	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. <b>Reference: CVE-2016-</b> 4119		
Coldfusion Adobe ColdF coding tasks		ed and	l tested application server t	hat simplifies	s complex
	2016-09-		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. <b>Reference: CVE-2016-</b>	https://hel px.adobe. com/secur ity/product s/coldfusio n/apsb16-	A-ADO- COLDF-
NA	01	6.4	4264	30.html	210916/11
Flash platfor	Player is fre	viewi	e software for using conte ng multimedia, executing r		

anu sueanni	ig video and	auun	<i>,</i>		
Execute	2016-09-	10	Use-after-free	https://hel	A-ADO-
Code	14		vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows	px.adobe. com/secur ity/product s/flash- player/aps	FLASH- 210916/12
			and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability	b16- 29.html	

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. <b>Reference: CVE-2016-</b> 6932		
Execute Code Execute Code	2016-09- 14 2016-09- 14	<u>10</u> 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, and CVE-2016-6930, and CVE-2016-6932. <b>Reference: CVE-2016-</b> <b>6931</b> 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://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/13 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. <b>Reference: CVE-2016-</b> 6930		
Execute Code Execute Code	2016-09- 14 2016-09- 14	<u>10</u> 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- 6930, CVE-2016-6931, and CVE-2016-6931, and CVE-2016-6932. <b>Reference: CVE-2016-</b> 6929 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://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/15 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. <b>Reference: CVE-2016-</b> 6927		
Execute Code Execute Code	2016-09- 14 2016-09- 14	10 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-2016-6931, and CVE-2016-6932. <b>Reference: CVE-2016- 6926</b> 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://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/17 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. <b>Reference: CVE-2016-</b> <b>6925</b>		
Denial of Service; Execute Code; Overflow; Memory Corruption Execute Code	2016-09- 14 2016-09- 14	10 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. <b>Reference: CVE-2016- 6924</b> 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://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/19 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. <b>Reference: CVE-2016-</b> 6923		
Denial of Service; Execute Code; Overflow; Memory Corruption Execute Code	2016-09- 14 2016-09- 14	<u>10</u> 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. <b>Reference: CVE-2016-</b> <b>6922</b> 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://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/21 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. <b>Reference: CVE-2016-</b> 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. <b>Reference: CVE-2016-</b> 4287	https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/23
			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-		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09- 14	10	2016-4276, CVE-2016- 4280, CVE-2016-4281, CVE-2016-4282, CVE- 2016-4283, CVE-2016- 4284, CVE-2016-6922, and CVE-2016-6924. <b>Reference: CVE-2016-</b> 4285	https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/24

/ <b>0-1 1-2 2-</b> coring <b>0-1 1-2 2-</b> cale	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. <b>Reference: CVE-2016-</b> <b>4284</b>	https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 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. <b>Reference: CVE-2016-</b> <b>4283</b>	https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 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. <b>Reference: CVE-2016-</b> <b>4282</b>	https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 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. <b>Reference: CVE-2016-</b> 4281	https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 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
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

			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-	https://hel	
Denial of			4281, CVE-2016-4282,	px.adobe.	
Service;			CVE-2016-4283, CVE-	com/secur	
Execute			2016-4284, CVE-2016-	ity/product	
Code;			4285, CVE-2016-6922,	s/flash-	
Overflow;			and CVE-2016-6924.	player/aps	A-ADO-
Memory	2016-09-		Reference: CVE-2016-	b16-	FLASH-
Corruption	14	10	4280	29.html	210916/29
			Use-after-free		
			vulnerability in Adobe		
			Flash Player before		
			Flash Player before 18.0.0.375 and 19.x		
			Flash Player before 18.0.0.375 and 19.x through 23.x before		
			Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows		
			Flash Player before 18.0.0.375 and 19.x through 23.x before		
			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		
			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		
			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		
			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		
			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,		
			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-	https://bol	
			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-	https://hel	
			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,	px.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-		
			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-	px.adobe. com/secur	
			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-	px.adobe. com/secur ity/product	A-ADO-
Execute	2016-09-		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. <b>Reference: CVE-2016-</b>	px.adobe. com/secur ity/product s/flash- player/aps b16-	FLASH-
Execute Code	2016-09- 14	10	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.	px.adobe. com/secur ity/product s/flash- player/aps	

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. <b>Reference: CVE-2016-</b> 4278	https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/31
Bypass; Gain Information Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09- 14 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. <b>Reference: CVE-2016- 4277</b> 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://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/32 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. <b>Reference: CVE-2016-</b> 4276		
Denial of Service; Execute Code; Overflow; Memory Corruption Denial of Service; Execute Code; Overflow; Memory Corruption	2016-09- 14 2016-09- 14	10 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. <b>Reference: CVE-2016-</b> 4275 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://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/34 A-ADO- FLASH- 210916/35

CV Scoring Scale	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. <b>Reference: CVE-2016-</b> 4274		
Execute Code Bypass; Gain Information	2016-09- 14 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-2016-6931, and CVE-2016-6932. <b>Reference: CVE-2016-</b> 4272 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://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html https://hel px.adobe. com/secur ity/product s/flash- player/aps b16- 29.html	A-ADO- FLASH- 210916/36 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 Soft				1	Ļ
Visual Nove			, , , .		.,
			al novel producing company	emerged fro	m the
former doujir	T CITCIE AKAD	ei 501		1	
			AKABEi SOFT2 games allow remote attackers to		
			execute arbitrary OS		
			commands via crafted		
			saved data, as	http://jvn.j	
			demonstrated by Happy	p/en/jp/JV	
			Wardrobe.	N8521341	A-AKA-
Execute	2016-09-		Reference: CVE-2016-	2/995740/i	VISUA-
Code	01	6.8	4853	ndex.html	210916/38
Aki-null					
Yorufukuro	u: NA			T	1
			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	http://jvn.j	
			crafted emoji character	p/en/jp/JV	
			sequence.	N9481636	A-AKI-
Denial of	2016-09-	4 3	Reference: CVE-2016-	1/995844/i	YORUF-
Service	12	4.3	4852	ndex.html	210916/39
Apache					
Openmeeti					
Jpenmeeting	gs provides	viae	o conferencing, instant m	iessaging, w	inite board

*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 (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. <b>Reference: CVE-2016-</b> <b>3089</b> enforcing fine grained role b a hadoop cluster. Multiple incomplete blacklist vulnerabilities in	http://ope nmeetings .apache.or g/security. html	A-APA- OPENM- 210916/40		
Safari/Chro Safari / Chr	me/Edge; Ir	ntern / 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. <b>Reference: CVE-2016- 0760</b> <b>lozilla; Opera</b> <b>et Explorer/Firefox/Opera</b> <i>ternet Explorer / Firefox /</i> <i>ram that provides a way to</i>	Opera are			
				IUUK at anu i			
all the information on the World Wide Web).Gain2016-09-5The 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"NAA-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		
			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.		A-APP-
Gain	2016-09-	_	Reference: CVE-2016-		SAFAR-
Information Cisco	06	5	7152	NA	210916/43
	ecurity App	lianc	e Software		
			enterprise-class security c	apabilities f	or the ASA
	ily in a variet				
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. <b>Reference: CVE-2016-</b> 6367	http://tool s.cisco.co m/security /center/vie wErp.x? alertId=ER P-56516	A-CIS- ADAPT- 210916/44
	ess Point S	oftwa			
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://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-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

CV Scoring	0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10
Gain Privileges	20	016-08- 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					tp://tool cisco.co /security enter/co ent/Cisc securityA	210	IS- 'CO- 916/48
This softwa network, fr user and e	are is u om an ndpoin	sed to g y device t behav	give ar e, at ar ior wit	ny user h ny time, h full vis	in any le sibility a	ocation cross th	and ne ex	to <u>:</u> ten	gain mo ded ent	re insi erprise	ght into e
	rt Ser							dð	μ	210	910/4/
Gain Privileges	20	016-08- 22 016-08- 22	7.2 6.1	CSCva0 Reference 6363 Cisco Aii and 380 software 8.2.12x and 8.3 8.3.102 users to via craft parame CSCu22 Reference 6362 The Agg Protocol (AMPDU on Cisco 2800, aii with sof 8.2.121 before 8 remote a denial reload) AMPDU ID CSCu Reference 6361	6192. nce: CV ronet 18 0 device before 8 before 8 0 allow 0 gain pr ced CLI ters, aka 4725. nce: CV regatec 1 Data U 1) impler 0 Airone nd 3800 tware be 0 and 8 3.3.102.0 attacker of servivia a cra header, 1256288	<b>E-201</b> <b>3</b> 00, 28 es with 8.2.110 <b>3</b> .2.121 e <b>1</b> ocal ivileges <b>a</b> Bug II <b>E-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-2010</b> <b>TE-20</b>	00, 0.0, .0, 5 0 <b>6-</b> on s use vice ig	aa ht: s.c n/ /ce nt oS dv co 20 aa ht: s.c n/ /ce nt oS dv co	tp://tool cisco.co /security enter/co ent/Cisc -sa- 160817 p1 tp://tool cisco.co /security enter/co ent/Cisc security enter/co ent/Cisc security fisory/cis -sa- 160817	A-C AIR( 210	ON- 916/46  S-
				attacker denial o reload) frames,	f service via craft aka Bug	e (devio ed 802					

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 crafted ID CSCu <b>Refere</b> 6369	INF file, 1292464 nce: CV	aka Bu ' <b>E-201</b> 0	ıg <b>6-</b>	dvisory/cis co-sa- 20160824 anyconneo t	-	
	<b>Policy Infra</b> vides central								
Through pro	grammability s opportuniti	, auto							
Execute Code	2016-08- 18	8.5	The Gra process Applicat Infrastru Enterpr EM) 1.0 authent execute comma crafted parame CSCux1 <b>Refere</b> 1365	in Cisco cion Poli- ucture C ise Modu allows n icated u arbitra nds as r upgrade ter, aka 5507.	o cy ontrolle ule (API remote sers to cy oot via e Bug ID	er IC- a <b>6-</b>	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurity dvisory/cis co-sa- 20160817 apic	A A-CI - APP	-
	<b>Streaming</b> Streaming A			A) is a	n anal	ytics	platform		delivers ionable
_	n high-veloc vernance and	-			ata froi	т ти	ltiple sour	ces, e	nabling
Gain Information	2016-08- 22	4	Cisco Co Streami allows r authent discove service reading pages, a CSCuz9 <b>Refere</b> 1477	onnecte ng Anal emote icated u r a notif passwo adminis aka Bug 2891.	ytics 1. sers to ication d by strative ID	6-	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurity dvisory/cis co-sa- 20160810 csa	A A-CI - CON	
· · · · · · · · · · · · · · · · · · ·	Managemer lanagement			es com	olete a	nd un	ified man	aneme	nt over
firewalls, ap malware pro	pplication col otection. Firep tover firewa	ntrol, power	intrusio Manage	n preve ement C	ntion, enter p	URL i provide	filtering, a es comple	nd ad te and	vanced unified
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.

and advan	ced ma	alware p	protect	ion.								
		016-08- 18		The well Cisco Fi Manage and 5.x 5.3.1.x and 5.4 and Cisc Security Softwar devices Services before 5 before 5 before 5 remote users to account crafted aka Bug	repower ment Co before 5 before 5 x before co Adap Applian e on 550 with Fir 5 4.x and 5.3.0.3, 5.3.1.2, 5.4.0.1 a authent o increas	enter 4 5.3.0.3, 5.3.1.2, e 5.4.0. tive nce (AS 00-X ePOWE d 5.x 5.3.1.x and 5.4 illows icated se user- ges via quests, ur2548	1 A) R .x	cis ec te /C rit y/c 20	tp://tool sco.com :urity/ce r/conter iscoSecu yAdviso cisco-sa 0160817 epower	/s n it u r - ,	A-CI FIRE 210	
Execute Code	2(	016-08- <u>18</u>		Manage and 5.x and 5.4 and Cisc Security Softwar devices Services before 5 before 5 before 5 remote users to comma crafted aka Bug	repower ment Co before 5 .x before co Adap / Appliar e on 550 with Fir s 4.x and 5.3.1.2 a 5.4.0.1 a authent o execut nds as r	enter 4 5.3.1.2 e 5.4.0. tive nce (AS 00-X ePOWE d 5.x ind 5.4. illows icated e arbitr oot via quests, ur2551	1 A) R x ary 3.	ht cis ec /C rit y/	tp://tool sco.com urity/ce r/conter iscoSecu yAdviso cisco-sa 0160817	/s n it u r - ,	A-CI FIRE 210	
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8	9-9	9-10

Cross-site scripting	2016-08- 22 <b>ystem Softv</b>	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. <b>Reference: CVE-2016-</b> 6365	http://tools. cisco.com/s ecurity/cen ter/content /CiscoSecu rityAdvisor y/cisco-sa- 20160817- firepowerm c	A-CIS- FIREP- 210916/53
Cisco Fires			oftware centralizes, inte	grates, and	simplifies
			tem Software provides		
			application control, and ir re protection.	itrusion prev	ention, ORL
Bypass Cross-site scripting	2016-09- 12 2016-09- 12	<u>5</u> 3.5	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. <b>Reference: CVE-2016- 6396</b> Cross-site scripting (XSS) vulnerability in the web- based management interface in Cisco Firepower Management Center before 6.1 and	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160907- fsss1 http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA	A-CIS- FIRES- 210916/54 A-CIS- FIRES- 210916/55
CV			FireSIGHT System Software before 6.1 allows remote authenticated users to inject arbitrary web script or HTML via a	dvisory/cis co-sa- 20160907- fsss	

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

Session fixationhttp://toolvulnerability in Ciscos. cisco.coFirepower Management			crafted URL, aka Bug ID CSCuz58658. Reference: CVE-2016- 6395		
Through Cisco Hosted Collaboration Mediation, NOC operators use a single dashboard that aggregates alarms from underlying domain managers.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 		12	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. <b>Reference: CVE-2016-</b> 6394	s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160907-	FIRES-
dashboard that aggregates alarms from underlying domain managers.dashboard that aggregates alarms from underlying domain managers.Directory traversalhttp://toolvulnerability in the webs.cisco.cointerface in Cisco HostedCollaboration Mediation/center/coFulfillment (HCM-F)ntent/Cisc10.6(3) and earlier allowsoSecurityAdvisory/cisremote attackers to writeto arbitrary files via aco-sa-crafted URL, aka Bug ID2016-09-Traversal1256371Directory2016-09-4Vulnerability in the webinterface in Cisco Hostedmylored attackers to writeto arbitrary files via aco-sa-crafted URL, aka Bug ID2016-09-4Vulnerability in the webinterface in Cisco Hostedmylored collaboration Mediation/center/cofulfillment (HCM-F)ntent/Cisc10.6(3) and earlier allowsoSecurityAdvisory/cisusers to read arbitraryco-sa-gather to read arbitraryco-sa-files via a craftedpathname in an HTTPrequest, aka Bug IDCSCuz27255.cocurityA					
Directory traversal vulnerability in the web interface in Cisco Hosted (Center/Co ntent/Cisc 0 SecurityA dvisory/cis co-sa- 2106-09- TraversalDirectory traversal vulnerability in the web interface in Cisco Hosted (Center/Co ntent/Cisc o SecurityA dvisory/cis co-sa- 210916/57A-CIS- HOSTE- 210916/57Directory Traversal2016-09- 125AA-CIS- HOSTE- 210916/57Directory Traversal2016-09- 124Directory traversal of G371http://tool s.cisco.co m/security /center/Co oSecurityAA-CIS- HOSTE- 210916/57Directory Traversal2016-09- 124Directory traversal olicetory traversal niterface in Cisco Hosted 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.http://tool s.cisco.co of Moster- 					se a single
	Traversal Directory	12 2016-09-	 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. <b>Reference: CVE-2016-</b> <b>6371</b> 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.	s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- hcmf http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831-	HOSTE- 210916/57 A-CIS- HOSTE-

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

			6370							
	rvices Engir									
			(ISE) is a network administra							
enables the creation and enforcement of security and access policies for endpoint										
devices conr	nected to the	comp	pany's routers and switches.	1						
			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	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA						
			parameters, aka Bug ID	dvisory/cis						
Conservation alternation	2010 00		CSCva46497.	co-sa-	A-CIS-					
Cross-site	2016-08- 22	12	Reference: CVE-2016- 1485	20160817- ise	IDENT- 210916/59					
scripting				ISE	210910/39					
The Cisco Me		ion Sy	suite stem (MOS) provides critica edia for multi-screen consur		equired to					
	2016-09-		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. <b>Reference: CVE-2016-</b>	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831-	A-CIS- MEDIA-					
Bypass	03	6.8	6377	vmp	210916/60					
Cisco Small I	Business 220	Serie	<b>Smart Plus Switches</b> as Smart Plus Switches bridg to offer customers the best o	<b>U</b> ,						
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://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-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 Busir	ness 220 Se	ries S	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. <b>Reference: CVE-2016-</b> <b>1472</b>	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-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. <b>Reference: CVE-2016-</b> 1471	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-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. <b>Reference: CVE-2016-</b> 1470	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- sps	A-CIS- SMALL- 210916/64							
CV Scoring Scale	0-1 1-2	2-3	<b>3-4 4-5 5-6</b> 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.											
<u>IIIessayes se</u>	curery, using		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.	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa-	A-CIS-						
Cross-site	2016-08-		Reference: CVE-2016-	20160817-	TRANS-						
scripting	22	4.3	6359	sch	210916/65						
	Unified Communications Manager										
UCM brings t	ogether SSL	VPN,	security, application acceler	ation, and av	ailability.						
	2016-08- 22 <b>tings Serve</b>		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. <b>Reference: CVE-2016- 6364</b>	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160817- ucm	A-CIS- UNIFI- 210916/66						
			ing through a web browser w		onferencing						
and video, so Bypass; Gain Information	<mark>o everyone s</mark> 2016-08- 22	ees th	the same thing while you talk Cisco WebEx Meetings Server 2.6 allows remote attackers to bypass intended access restrictions and obtain sensitive application information via unspecified vectors, aka	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa-	A-CIS- WEBEX- 210916/67						
CV Scoring Scale	CV Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10										

	• <b>Player T29</b> bFx Player vo	ou car	Bug ID CSCuy92724. <b>Reference: CVE-2016- 1484</b> watch, share, and edit Web	20160817- wms1	15.
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. <b>Reference: CVE-2016- 1464</b>	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-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. <b>Reference: CVE-2016-</b> 1415	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- webex	A-CIS- WEBEX- 210916/69
Controller 7.2;Wireles	7.0;Wireless ss LAN Cont V Controller o	5 LAN rollei	reless LAN Controller 6.0, I Controller 7.1;Wireless I r 7.4 zes the performance of your	LAN Control	ller

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

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- 01	4.3	Cross-site scripting (XSS)https://gitA-CLI-vulnerability in ClipBuckethub.com/aCLIPB-before 2.8.1 RC2 allowsrslancb/cli210916/72remote attackers to injectpbucket/c								
Clip-Bucket and we do s every step o & Audios to Friends, Mes	<b>Clip-bucket</b> 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.										
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. <b>Reference: CVE-2016-</b> 6493	http://sup port.citrix. com/articl e/CTX215 460	A-CIT- XENAP- 210916/71						
Xenapp; Xenapp allow Shared serve that allows r installed at a	<b>Citrix</b> <b>Xenapp; Xendesktop</b> <i>Xenapp allows Windows applications to be accessed via individual devices from a</i> <i>shared server or cloud system; XenDesktop is a desktop virtualization software</i> <i>that allows multiple users to access and run Microsoft Windows desktops that are</i> <i>installed at a centralized location separate from the devices from which they are</i> <i>being accessed.</i>										
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. <b>Reference: CVE-2016- 6376</b>	http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- wlc-2	A-CIS- WIREL- 210916/70						

	Т				1							
				ommit/ff5								
			arbitrary web script or	e37d3e10								
			HTML via unspecified	98a7ce2b								
			vectors.	9fe60389b								
			Reference: CVE-2016-	14514932								
			4848	dd93								
Dotnetnuke	uu 95											
Dotnetnuke is the leading open source web content management platform (CMS) in												
	t ecosystem.	, -  :		,	( ( ,							
			Cross-site scripting (XSS)									
			vulnerability in the user-									
			profile biography section									
			in DotNetNuke (DNN)									
			before 8.0.1 allows									
			remote authenticated	http://www								
			users to inject arbitrary	.dnnsoftw								
			web script or HTML via a	are.com/c								
			crafted onclick attribute in	ommunity/								
			an IMG element.	security/s	A-DOT-							
Cross-site	2016-08-		Reference: CVE-2016-	ecurity-	DOTNE-							
scripting	31	3.5	7119	center	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.												
experiences.	. σταρά ριον	lues c	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									
			-									
			might allow remote authenticated users to									
			might allow remote authenticated users to bypass intended access									
			might allow remote authenticated users to bypass intended access restrictions and obtain	https://ww								
			might allow remote authenticated users to bypass intended access	https://ww w.drupal.o								
Bynass:			might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via	w.drupal.o	A-DRU-							
Bypass; Gain	2016-09-		might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors.	w.drupal.o rg/SA-	A-DRU- DRUPA-							
Gain	2016-09-	Ę	might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors. <b>Reference: CVE-2016-</b>	w.drupal.o rg/SA- CORE-	DRUPA-							
Gain Information	2016-09- 09	5	might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors.	w.drupal.o rg/SA-								
Gain Information EMC	09		might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors. <b>Reference: CVE-2016-</b> 6212	w.drupal.o rg/SA- CORE-	DRUPA-							
Gain Information EMC Authentica	09 tion Manage	er Pr	might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors. <b>Reference: CVE-2016-</b> 6212 ime Self-service	w.drupal.o rg/SA- CORE- 2016-002	DRUPA- 210916/74							
Gain Information EMC Authentica RSA Auther	09 tion Manage	<mark>er Pr</mark> nagei	might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors. <b>Reference: CVE-2016-</b> 6212 ime Self-service r: Platform behind RSA S	w.drupal.o rg/SA- CORE- 2016-002	DRUPA- 210916/74							
Gain Information EMC Authentica RSA Auther centralized r	09 <b>tion Manage</b> ntication Man management	er Pr nager of th	might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors. <b>Reference: CVE-2016-</b> 6212 <b>ime Self-service</b> <i>:: Platform behind RSA State RSA SecurID environment</i>	w.drupal.o rg/SA- CORE- 2016-002	DRUPA- 210916/74							
Gain Information EMC Authentica RSA Auther centralized r methods, us	09 <b>tion Manag</b> ntication Management management sers, applicat	<b>er Pr</b> nager of th ions,	might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors. <b>Reference: CVE-2016-</b> 6212 ime Self-service r: Platform behind RSA S re RSA SecurID environment and agents across multiple	w.drupal.o rg/SA- CORE- 2016-002	DRUPA- 210916/74 allows for thentication es. It verifies							
Gain Information EMC Authentica RSA Auther centralized r methods, us	09 <b>tion Manag</b> ntication Management management sers, applicat	<b>er Pr</b> nager of th ions,	might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors. <b>Reference: CVE-2016-</b> 6212 <b>ime Self-service</b> <i>:: Platform behind RSA State RSA SecurID environment</i>	w.drupal.o rg/SA- CORE- 2016-002	DRUPA- 210916/74 allows for thentication es. It verifies							
Gain Information EMC Authentica RSA Auther centralized r methods, us authenticatio	09 tion Manage ntication Management sers, application requests	er Pr nager of th ions, and	might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors. <b>Reference: CVE-2016-</b> 6212 ime Self-service r: Platform behind RSA St re RSA SecurID environment and agents across multiple centrally administers auto	w.drupal.o rg/SA- CORE- 2016-002	DRUPA- 210916/74 allows for thentication es. It verifies policies for							
Gain Information EMC Authentica RSA Auther centralized r methods, us authenticatio	09 <b>tion Manag</b> ntication Management management sers, applicat	<b>er Pr</b> nager of th ions,	might allow remote authenticated users to bypass intended access restrictions and obtain sensitive Statistics information via unspecified vectors. <b>Reference: CVE-2016-</b> 6212 ime Self-service r: Platform behind RSA St re RSA SecurID environment and agents across multiple centrally administers auto	w.drupal.o rg/SA- CORE- 2016-002	DRUPA- 210916/74							

organizations' end users.											
Denial of Service		016-08- 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." <b>Reference: CVE-2016- 0915</b>				st: gt	tp://secl s.org/bu raq/201 Aug/71	A-E AU	МС- ГНЕ- )916/75
GNU	_									<b>I</b>	-
Libidn				_							_
Libidn is dev	/elope	ed for th	ie GNL		ystem,	but run	s on	ove	er 20 Un	ix plat	forms.
Denial of Service	20	016-09- 07	5	The stringprep_utf8_nfkc_nor malize 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. <b>Reference: CVE-2016-</b> 6263			av nu /lil co id 7e 22 e4	tp://git.s vannah.g i.org/cgi bidn.git/ mmit/? =1fbee5 ef3c72dk 206dd87 162108 2f42555	a t A-G LIB	INU- ID- 0916/76	
Mailman				<i>c.</i>		c		~ • •			
					oplicatio	on from	the	GN	U Projec	t for	
managing e Cross Site Request Forgery		016-09- 02	ling lis	ftware application from the orbits. 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. <b>Reference: CVE-2016-</b>		gs ad	tps://bu s.launch l.net/bu 1614841	o MA g 210	iNU- ILM- )916/77		
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

			7123		
			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	https://bu	
Cross Site			of a victim's account.	gs.launchp	A-GNU-
Request Forgery	2016-09- 02	6.8	Reference: CVE-2016- 6893	ad.net/bug s/1614841	MAILM- 210916/78
Google					
Chrome					
Google Chrol	me is a freev	vare n	<mark>eb browser developed by G</mark> SkPath.cpp in Skia, as	oogle.	
			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	https://cod ereview.chr	
			via crafted graphics data.	omium.org/	A-G00-
Denial of Service	2016-09- 11	6.8	Reference: CVE-2016- 7395	200614300 9	CHROM-
Denial of	2016-09-	7.5	Multiple unspecified	9 https://goo	210916/79 A-GOO-
Service	11		vulnerabilities in Google	glechromer	CHROM-
			Chrome before 53.0.2785.89 on	eleases.blo gspot.com/	210916/80
			Windows and OS X and	2016/08/st	
CV	0-1 1-2	2-3	3-4 4-5 5-6 6	-7 7-8	8-9 9-10
Scoring Scale					

			before 53.0.2785.92 on Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors. <b>Reference: CVE-2016-</b> <b>5167</b>	able- channel- update-for- desktop_31 .html	
Gain Information Cross-site scripting	2016-09- 11 2016-09- 11	2.6 4.3	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. <b>Reference: CVE-2016- 5166</b> 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://goo glechromer eleases.blo gspot.com/ 2016/08/st able- channel- update-for- desktop_31 .html https://goo glechromer eleases.blo gspot.com/ 2016/08/st able- channel- update-for- desktop_31 .html	A-GOO- CHROM- 210916/81 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-	4.3	Cross-site scripting (XSS) vulnerability in WebKit/Source/platform/v 8_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)." <b>Reference: CVE-2016-</b> <b>5164</b>	https://goo glechromer eleases.blo gspot.com/ 2016/08/st able- channel- update-for- desktop_31 .html	A-GOO- CHROM- 210916/83
	2016-09-	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. <b>Reference: CVE-2016-</b> <b>5163</b>	https://goo glechromer eleases.blo gspot.com/ 2016/08/st able- channel- update-for- desktop_31 .html	A-GOO- CHROM- 210916/84
NA	2016-09-	4.3	The	https://goo	A-G00-

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

			urceLoa extensio quest_u Chrome 53.0.27 Window before 5 Linux do use an e manifes web_aco s field fo IFRAME makes i remote conduct attacks, into cha settings web site vulneral 2016-51 <b>Referen</b> 5162	ons/brow til.cc in before 85.89 of s and O 53.0.278 oes not extension tessible or restric elemen t easier attacket clickjac and tric nging e s, via a c e, a diffe bility tha 60.	vser/url Google S X and 5.92 or properly n's _resour ctions o ts, whic for rs to cking ck users xtensio rafted erent an CVE-	- h y ce n ch	gsp 201 abl cha upo	annel- date-for- sktop_31		916/85
Denial of Service	2016-09- 11	6.8	The EditingS function WebKit/ ng/Editi Blink, as Chrome 53.0.27 Window before 5 Linux, n custom allows r to cause service unspeci via a cra that lev confusio StylePro class.	n in Source/ongStyle s used in before 85.89 of 53.0.278 nishandl propert emote a e a deni or possi fied oth afted we erages ' on" in th	core/ed cpp in n Googl n S X and 5.92 or es ies, whi ittacker al of bly hav er impa eb site 'type e	iti e h ich rs re	gle ele gsp 202 abl cha upo	annel- date-for- sktop_31	CHR 210	OO- OM- 916/86
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 Denial of Service;	2016-09- 11 2016-09- 11	<u>4.3</u> 6.8	The AllowCrossRendererReso urceLoad function in extensions/browser/url_re quest_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_resource s 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. <b>Reference: CVE-2016-</b> 5160 Multiple integer overflows in OpenJPEG,	https://goo glechromer eleases.blo gspot.com/ 2016/08/st able- channel- update-for- desktop_31 .html https://goo glechromer	A-GOO- CHROM- 210916/87 A-GOO- CHROM-
Overflow	11		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	eleases.blo gspot.com/ 2016/08/st able- channel- update-for- desktop_31 .html	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
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

5159       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.https://crbuA-G	00- 100-
Overflow         11         6.8         5158         890         210	916/89
Overflow         11         6.8         5157         178ea9         210           Denial of         2016-09-         6.8         extensions/renderer/even         https://goo         A-G	COM- 916/90
	ЮМ- 916/91

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. <b>Reference: CVE-2016-</b> <b>5156</b>	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. <b>Reference: CVE-2016-</b> <b>5155</b>	https://goo glechromer eleases.blo gspot.com/ 2016/08/st able- channel- update-for- desktop_31 .html	A-GOO- CHROM- 210916/92
Denial of Service Overflow Denial of Service	2016-09- 11 2016-09- 11	<u>6.8</u> 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. <b>Reference: CVE-2016- 5154</b> The Web Animations implementation in Blink,	https://goo glechromer eleases.blo gspot.com/ 2016/08/st able- channel- update-for- desktop_31 .html https://goo glechromer	A-GOO- CHROM- 210916/93 A-GOO- CHROM-
Service			implementation in Blink, as used in Google Chrome before	glechromer eleases.blo gspot.com/	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. <b>Reference: CVE-2016-</b> 5153	2016/08/st able- channel- update-for- desktop_31 .html	
Denial of Service Overflow Denial of Service	2016-09- 11 2016-09- 11	<u>6.8</u> 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. <b>Reference: CVE-2016- 5152</b> 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://goo glechromer eleases.blo gspot.com/ 2016/08/st able- channel- update-for- desktop_31 .html https://crbu g.com/634 716	A-GOO- CHROM- 210916/95 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
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Denial of	2016-09-	6.8	document, related to fpdfsdk/javascript/JS_Obj ect.cpp and fpdfsdk/javascript/app.cp p. <b>Reference: CVE-2016- 5151</b> WebKit/Source/bindings/ modules/v8/V8BindingFor Modules.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. <b>Reference: CVE-2016-</b> 5150	https://cod ereview.chr omium.org/ 225541300	A-GOO- CHROM- 210916/97
Service NA	11 2016-09-	6.8 6.8	<b>5150</b> The extensions	4/ https://cod	210916/97 A-GOO-
	11	0.0	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	ereview.chr omium.org/ 220848300 2/	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)." <b>Reference: CVE-2016-</b> <b>5148</b>	https://cod ereview.chr omium.org/ 213411300 2	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)." <b>Reference: CVE-2016-</b> <b>5147</b>	https://cod ereview.chr omium.org/ 215539300 2	A-GOO- CHROM- 210916/10 0
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). <b>Reference: CVE-2016-</b> <b>5430</b>	https://git hub.com/n ov/jose- php/comm it/f03b986 b4439e20 b0fd63510 9b48afe96 cf0099b# diff- 37b0d289 d6375ba4 a7740401 950ccdd6 R199	A-GRE- JOSE 210916/10 1
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. <b>Reference: CVE-2016-</b> <b>5429</b>	https://gith ub.com/nov /jose- php/commi t/f03b986b 4439e20b0 fd635109b 48afe96cf0 099b#diff- 37b0d289d 6375ba4a7 740401950 ccdd6R287	A-GRE- JOSE 210916/10 2

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	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.

weight need	s for HPE Syr	iergy	solutions.		
			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	https://h	
			for Microsoft SharePoint	20566.w	
			2010 before 16.11.1, and	ww2.hp	
			Sizer for Microsoft Skype for		
			Business Server 2015 before		
			16.5.1 allows remote	public/di	
			attackers to execute	splay?	
			arbitrary code via	docld=e	A-HP-
	2016 00		unspecified vectors.	mr_na-	CONVE-
Execute	2016-08-		Reference: CVE-2016-	c05237	210916/10
Code	22	7.6	4377	578	3
Operations		6		<i>с</i> , , ,	
		s a Sy	stem monitoring package ma	anufactured	by Hewlett-
Packard (HP)		2 5		http://b-2	
Cross-site	2016-09-	3.5	Cross-site scripting (XSS)	https://h2	A-HP-
scripting	08		vulnerability in the AdminUI in HPE	0566.www	OPERA-
				2.hpe.com	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

**Operations Manager** 

/portal/site

4

HP XP P9000	Command V	iew A	<ul> <li>9.21.x before 9.21.130 <ul> <li>allows remote</li> <li>authenticated users to</li> <li>inject arbitrary web script</li> <li>or HTML via unspecified</li> <li>vectors.</li> </ul> </li> <li>Reference: CVE-2016-4380</li> <li>O7 Command View</li> <li>Advanced Edition Software is and XP Disk Array products.</li> </ul>	/hpsc/publ ic/kb/docD isplay? docId=em r_na- c0524983 3	ed device
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. <b>Reference: CVE-2016-</b> <b>4378</b>	https://h2 0566.www 2.hpe.com /portal/site /hpsc/publ ic/kb/docD isplay? docId=em r_na- c0524135 5	A-HP-XP 90- 210916/10 5
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. <b>Reference: CVE-2016-</b> <b>4381</b>	https://h2 0566.www 2.hpe.com /portal/site /hpsc/publ ic/kb/docD isplay? docId=em r_na- c0525771 1	A-HP-XP7 C- 210916/10 6
Bypass Huawei	08	4.4	4381	1	6

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

E9000 Chas	sis				
			verged-architecture blade se		
convergence	e of computin	g, sto	prage, networking, and mana	agement.	
			XML external entity (XXE)		
			vulnerability in the Hyper		
			Management Module		
			(HMM) in Huawei E9000		
			rack servers with software		
			before	<b>b b b b c c ( f c c c c c c c c c c</b>	
			V100R001C00SPC296	http://www .huawei.co	
			allows remote authenticated users to	m/en/psirt	
			read arbitrary files or	/security-	
			cause a denial of service	advisories/	
			(web service outage) via	huawei-sa-	A-HUA-
			a crafted XML document.	20160824-	E9000-
Denial of	2016-09-		Reference: CVE-2016-	01-e9000-	210916/10
Service	07	4.9	6898	en	7
Fusionacce				0.1	-
		irtuali	zes and centralizes PC o	computing a	and storage
			reating a Virtual Desktop Inf		-
			CRLF injection		
			vulnerability in Huawei	http://www	
			FusionAccess before	.huawei.co	
			V100R006C00 allows	m/en/psirt	
			remote attackers to inject	/security-	
			arbitrary HTTP headers	advisories/	
			and conduct HTTP	huawei-sa-	
			response splitting attacks	20160817-	A-HUA-
	2010 00		via unspecified vectors.	01-	FUSIO-
	2016-09-	4 2	Reference: CVE-2016-	fusionacce	210916/10
Http R.Spl.	07	4.3	6839	ss-en	8
	ified Mainter	nanco	Audit (IIMA) system centr	ally manage	s monitors
	ei's Unified Maintenance Audit (UMA) system centra adits operations of all Operation and Maintenance				
enterprise.			speration and maintenance	(out) per	
Execute	2016-09-	10	Huawei Unified	http://www	A-HUA-
Code	07		Maintenance Audit (UMA)	.huawei.co	UMA-
			before	m/en/psirt	210916/10
			V200R001C00SPC200	/security-	9
			allows remote attackers	advisories/	
			to execute arbitrary	huawei-sa-	
			commands via "special	20160824-	
			characters," a different	01-uma-	
CV					
Scoring	0-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10
Scale					

Gain Information2016-09- 07before V200R01C00SPC200 allows remote attackers to execute arbitrary commands via "special characters," a different 2016-7110.http://www .huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160824- 01-uma-A-HUA 20160824- UMA- 20160824- 01-uma- 0Execute Code2016-09- 07107109en0Huawei Unified before V200R001C00SPC200 SPH206 allows remote authenticated users to obtain the MD5 hashes of arbitrary user passwords via unspecified vectors.http://www .huawei-sa- 20160824- 02-uma- advisories/ advisories/ atvisories/ authenticated users to obtain the MD5 hashes of arbitrary user passwords via unspecified vectors.A-HUA enGain Information2016-09- 4Reference: CVE-2016- authenticated users to obtain the MD5 hashes of arbitrary user passwords via unspecified vectors.02-uma- enGain Information2016-09- 4Huawei Unified Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 SPH206 allows remote attackers to reset and consequently affecthttp://www .huawei.co m/en/psirt i security-			Reference: CVE-2016- 7110 Huawei Unified	en	
Gain2016-09- InformationMaintenance Audit (UMA) before.huawei.co m/en/psirt sPH206 allows remote authenticated users to obtain the MD5 hashes of 		10	V200R001C00SPC200 allows remote attackers to execute arbitrary commands via "special characters," a different vulnerability than CVE- 2016-7110. <b>Reference: CVE-2016-</b> <b>7109</b>	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160824- 01-uma- en	210916/11
Gain Information2016-09- 07SPH206 allows remote authenticated users to obtain the MD5 hashes of arbitrary user passwords via unspecified vectors. Reference: CVE-2016- Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 SPH206 allows remote attackers to reset arbitrary user passwords Maintenance Audit (UMA) before V200R001C00SPC200 Attackers to reset arbitrary user passwords Maintenance Audit (UMA) before V200R001C00SPC200 Attackers to reset arbitrary user passwords attackers to reset arbitrary user passwords attackers to reset and consequently affectadvisories/ advisories/ advisories/ advisories/			Maintenance Audit (UMA) before	.huawei.co m/en/psirt	
Gain Information2016-09- 07via unspecified vectors. Reference: CVE-2016- 7108enUMA- 21091 1Huawei Unified 			SPH206 allows remote authenticated users to	advisories/ huawei-sa-	
Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 http://www SPH206 allows remote .huawei.co attackers to reset m/en/psirt arbitrary user passwords /security- and consequently affect advisories/		4	via unspecified vectors. Reference: CVE-2016-		210916/11
unspecified vectors. 20160824- UMA-	2016-09-		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. <b>Reference: CVE-2016-</b>	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160824- 02-uma-	A-HUA- UMA- 210916/11

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. <b>Reference: CVE-2016- 0293</b> WebReports in IBM BigFix Platform (formerly Tivoli	http://ww w- 01.ibm.co m/support /docview. wss? uid=swg2 1985743	A-IBM- BIGFI- 210916/11 3
Gain Information	2016-08- 30	4.3	Endpoint Manager) 9.x before 9.5.2 allows remote attackers to obtain sensitive information by sniffing the network for HTTP traffic. <b>Reference: CVE-2016-</b> 0397	http://ww w- 01.ibm.co m/support /docview. wss? uid=swg2 1985907	A-IBM- BIGFI- 210916/11 4
Gain	2016-08- 30		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. <b>Reference: CVE-2016- 0292</b>	http://ww w- 01.ibm.co m/support /docview. wss? uid=swg2 1985907	A-IBM- BIGFI- 210916/11 5
Connection	IS				
	s' allows youı nd deliver re.		nization to engage the right	people, acce	elerate
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://ww w- 01.ibm.co m/support /docview. wss? uid=swg2 1988991	A-IBM- CONNE- 210916/11 6
CV Scoring Scale	0-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10

Cross-siteCross-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 scripti Or HTML via unspecified vectors, a different 2016-2954 and CVE-2016- 2956.http://ww w- Msupport A-IBM- CONNE- 210916/11 7Cross-site scripting2016-09- 3.5Reference: CVE-2016- 3.5Nulnerability than CVE- 2016-2954 and CVE-2016- 2956.A-IBM- CONNE- 210916/11 7Cross-site scripting2016-09- 3.5Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 4.0 through CR4, 4.5 through CR5, 5.0 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.A-IBM- CONNE- 210916/11 Reference: CVE-2016- 3.5Cross Site Scripting2016-09- 3.5SoosNulnerability m/support (CSRF) vulnerability in than CVE-2016-2995, CVE-2016-2995, CVE-2016-2997, and CVE- 2016-3010.A-IBM- CONNE- 210916/11 8Cross Site Request Forgery2016-09- 3.5SoosNulne- m/support (CSRF) vulnerability in IBM Connections 4.0 through CR4, 4.5 through CR5, 5.0 before CR4, and S.5 bef				unspecified vectors, a different vulnerability than CVE-2016-2995, CVE-2016-2997, and CVE- 2016-3005. <b>Reference: CVE-2016-</b> <b>3010</b>		
Cross-site scripting2016-09- scriptingCross-site request SiteCross-site request Site2016-09- SiteA-IBM- CONNE- CONNE- 210916/11Cross Site scripting2016-09- S.53.5Cross-site request forgery CSF, 5.0 before CR4, and S.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors, a W- 01.ibm.co 			3.5	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. <b>Reference: CVE-2016-</b>	w- 01.ibm.co m/support /docview. wss? uid=swg2	CONNE- 210916/11
ForgeryIBM Connections 4.001.ibm.co210916/11through CR4, 4.5 through CR5, 5.0 before CR4, and 5.5 before CR1 allowsm/support9	Cross-site scripting Cross Site	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. <b>Reference: CVE-2016-</b> <b>3005</b> Cross-site request forgery	http://ww w- 01.ibm.co m/support /docview. wss? uid=swg2 1988991	A-IBM- CONNE- 210916/11 8
	Request		3.5	(CSRF) vulnerability in IBM Connections 4.0 through CR4, 4.5 through CR5, 5.0 before CR4, and 5.5 before CR1 allows	w- 01.ibm.co m/support /docview. wss?	CONNE- 210916/11

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. <b>Reference: CVE-2016-</b> <b>2998</b>	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. <b>Reference: CVE-2016-</b> 2997	http://ww w- 01.ibm.co m/support /docview. wss? uid=swg2 1988991	A-IBM- CONNE- 210916/12 0
Cross-site scripting Cross-site scripting	2016-09- 01 2016-09- 01	<u>3.5</u> 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. <b>Reference: CVE-2016-</b> 2995 Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 5.0	http://ww w- 01.ibm.co m/support /docview. wss? uid=swg2 1988991 http://ww w- 01.ibm.co	A-IBM- CONNE- 210916/12 1 A-IBM- CONNE- 210916/12
			before CR4 and 5.5 before CR1 allows remote authenticated users to	m/support /docview. wss?	210910/12 2

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

CV Scoring Scale	0-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10
			Rational Team Concert 6.0.1 and 6.0.2 before 6.0.2 iFix2 and Rational Collaborative Lifecycle Management 6.0.1 and	01.ibm.co m/support /docview. wss? uid=swg2	210916/12 5
Cross-site scripting	2016-09- 12	3.5	Cross-site scripting (XSS) vulnerability in IBM	http://ww w-	A-IBM- RATIO-
IBM Rational managemen	Collaborativ	e Life at incl	cycle Management is an app udes IBM Rational Team Con	plication lifec	ycle
			ycle Management; Ratio		
Cross-site scripting Cross-site scripting	2016-09- 01 2016-08- 31	3.5 3.5	vectors, a different vulnerability than CVE- 2016-2954 and CVE-2016- 3008. <b>Reference: CVE-2016- 2956</b> 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. <b>Reference: CVE-2016-</b> 2954 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. <b>Reference: CVE-2016-</b> 0370	uid=swg2 1988990 http://ww w- 01.ibm.co m/support /docview. wss? uid=swg2 1988990 http://ww w- 01.ibm.co m/support /docview. wss? uid=swg2 1988726	A-IBM- CONNE- 210916/12 3
			inject arbitrary web script or HTML via unspecified		

Tivoli Storage Manager For Space Management to move inactive or seldom-used files to server storage, freeing disk space for active data.Image: Tivoli Storage Manager for Space Management to move inactive or seldom-used files to server storage, freeing disk space for active data.Image: Tivoli Storage Manager for Space Management to move inactive or seldom-used files to server storage, freeing disk space for active data.Image: Tivoli Storage Manager for Space Management (aka Spectrum Protect for Space Management) 6.3.x before 6.3.2.6, 6.4.x before 6.3.2.6, 6.4.x before 6.3.3.3, and 7.1.x before 7.1.6, when certain dsmsetpw tracing is encrypted password by reading application-trace output.Gain2016-09- 122.1SpaceSpaceMwebSphere Application ServerImagement CVE-2016- 1989006Image: Application Server is the leading open standards-based application operational efficiency, reliability, administration, security, and control.Overflow;2016-09- 3.53.5Buffer overflow in IBM were WESSphere Application Server10.100 12WebSphere Application Server10.100 10 10WebSphere Application Server10.100 10 10 10 10Overflow;2016-09- 3.53.5Buffer overflow in IBM were WESSphere Application4.18M WebSphere Application	
O3311989899Tivoli Storage Manager For Space Management to move inactive or seldom-used files to server storage, freeing disk space for active data.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 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.http://ww w- Verson discover an m/support /docview. A-IBM- TIVOL- uid=swg2 1989006Gain Information2016-09- 12Reference: CVE-2016- 12n/support 1989006WebSphere Application Server IBM WebSphere Application Server is the leading open standards-based application operational efficiency, reliability, administration, security, and control.A-IBM- Monvative applications and unmatch operational efficiency, reliability, administration, security, and control.	
Tivoli Storage Manager for Space Management to move inactive or seldom-used files to server storage, freeing disk space for active data.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.http://ww w- Management (docview. Wesphere Application ServerGain Information2016-09- 12Reference: CVE-2016- 1989006n/support 1989006WebSphere Application Server IbM WebSphere Application Server is the leading open standards-based applicat operational efficiency, reliability, administration, security, and control.A-IBM- Mttp://ww MA-IBM- Mttp://ww MA-IBM- Mttp://ww	
files to server storage, freeing disk space for active data.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.http://ww ws? TIVOL- uid=swg2 210916, 1989006Gain Information2016-09- 12Reference: CVE-2016- 15927w- Uid=swg2 1989006WebSphere Application Server IBM WebSphere Application Server is the leading open standards-based applicat foundation offering accelerated delivery of innovative applications and unmatch operational efficiency, reliability, administration, security, and control.Overflow;2016-09- 3.5Buffer overflow in IBMhttp://wwA-IBM-	
Gain Information2016-09- 12BM 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 encrypted password by reading application-trace output.http://ww w- Movie<	
Gain2016-09- InformationReference: CVE-2016- output.Manage 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 encrypted password by m/support reading application-trace output.Http://ww w- Version-trace docview. Management (aka A-IBM- Management) 6.3.x before 7.1.6, when certain dsmsetpw tracing is encrypted password by m/support reading application-trace output.A-IBM- M-IBM- ManagementGain2016-09- 122.1592719890066WebSphere Application Server IBM WebSphere Application Server is the leading open standards-based applicat foundation offering accelerated delivery of innovative applications and unmatch operational efficiency, reliability, administration, security, and control.A-IBM- M-IBM-Overflow;2016-09- 3.5Buffer overflow in IBMhttp://wwA-IBM-	
Gain2016-09- 12Z.1SpaceManagement (aka 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 encrypted password by reading application-trace output.http://ww w- MonoverGain2016-09- 12Reference: CVE-2016- 1989006w- m/support 1989006A-IBM- wss? TIVOL- 1989006Gain2016-09- 12Space 2.1Space space space space configured, allows local users to discover an encrypted password by reading application-trace output.A-IBM- wss? TIVOL- uid=swg2 1989006Gain2016-09- 12Space 2.1Space space space space output.A-IBM- wss?MwebSphereApplication ServerServer Space space space space space space space spaceA-IBM- wss?Overflow;2016-09- 3.53.5Buffer overflow in IBMhttp://wwA-IBM- wssA-IBM- wss?	
Gain2016-09- InformationReference: CVE-2016- output.with the system of the sy	
Gain2016-09- InformationReference: CVE-2016- Is the leading open standards-based applicationA-IBM- TIVOL- Uid=swg2BM WebSphere Application Server is the leading open standards-based applicationServer is the leading open standards-based application finnovative applications and unmatch operational efficiency, reliability, administration, security, and control.A-IBM- A-IBM- Metry	
Gain2016-09- InformationReference: CVE-2016- Is the leading open standards-based application defined and unmatch operational efficiency, reliability, administration, security, and control.A-IBM- A-IBM- Methylic the leading open standards-based application defined application in the leading open standards-based application definition in the leading open standards-based application definitio	
Gain2016-09- InformationA-IBM- 2.1S927A-IBM- 1989006WebSphere Application ServerServer is the leading open standards-based application output, administration, security, and control.A-IBM- With the security of t	
dsmsetpw tracing is configured, allows local users to discover an encrypted password by reading application-trace output.http://ww w- Misupport /docview.Gain Information2016-09- 12 <b>Reference: CVE-2016-</b> 1989006uid=swg2 1989006210916/ 6Websphere Application Server IBM WebSphere Application Server is the leading open standards-based applicat foundation offering accelerated delivery of innovative applications and unmatche operational efficiency, reliability, administration, security, and control.A-IBM- WebSphereOverflow;2016-09-3.5Buffer overflow in IBMhttp://wwA-IBM-	
Gain2016-09- InformationReference: CVE-2016- Informationw- 01.ibm.co m/supportGain2016-09- 122.1S92719890066Websphere Application Server IBM WebSphere Application Server is the leading open standards-based application operational efficiency, reliability, administration, security, and control.A-IBM- MeterOverflow;2016-09- 2.13.5Buffer overflow in IBMhttp://wwA-IBM-	
Gain2016-09-users to discover an encrypted password by reading application-trace output.01.ibm.co m/support /docview.A-IBM- VOL-Gain2016-09-Reference: CVE-2016- 1989006uid=swg2 1989006210916/ 1989006Information122.1592719890066Websphere Application ServerIBM WebSphere Application Server is the leading open standards-based application foundation offering accelerated delivery of innovative applications and unmatch operational efficiency, reliability, administration, security, and control.A-IBM-Overflow;2016-09-3.5Buffer overflow in IBMhttp://wwA-IBM-	
Gain2016-09- 1nformationencrypted password by reading application-trace output.m/support /docview. wss?A-IBM- TIVOL- uid=swg2Gain2016-09- 122.1Reference: CVE-2016- 5927uid=swg2210916/ 1989006Websphere Application Server592719890066Websphere Application Server is the leading open standards-based application foundation offering accelerated delivery of innovative applications and unmatch operational efficiency, reliability, administration, security, and control.Overflow;2016-09-3.5Buffer overflow in IBMhttp://wwA-IBM-	
Gain2016-09- 1nformationreading application-trace output./docview. wss?A-IBM- TIVOL- uid=swg2Gain2016-09- 12 <b>Reference: CVE-2016-</b> 1989006uid=swg2 1989006210916, 6Websphere Application ServerIBM WebSphere Application Server is the leading open standards-based applicat foundation offering accelerated delivery of innovative applications and unmatch operational efficiency, reliability, administration, security, and control.Overflow;2016-09-3.5Buffer overflow in IBMhttp://wwA-IBM-	
Gain Information2016-09- 12Reference: CVE-2016- 5927uid=swg2 1989006210916/ 6Websphere Application ServerServerServerServerIBM WebSphere Application Server is the leading open standards-based application foundation offering accelerated delivery of innovative applications and unmatch operational efficiency, reliability, administration, security, and control.Uid=swg2 1989006210916/ 6Overflow;2016-09-3.5Buffer overflow in IBMhttp://wwA-IBM-	
Information122.1592719890066Websphere Application ServerIBM WebSphere Application Server is the leading open standards-based applicatfoundation offering accelerated delivery of innovative applications and unmatchoperational efficiency, reliability, administration, security, and control.Overflow;2016-09-3.5Buffer overflow in IBMhttp://wwA-IBM-	
Websphere Application ServerIBM WebSphere Application Server is the leading open standards-based applicatfoundation offering accelerated delivery of innovative applications and unmatchoperational efficiency, reliability, administration, security, and control.Overflow;2016-09-3.5Buffer overflow in IBMhttp://wwA-IBM-	12
IBM WebSphere Application Server is the leading open standards-based applicat foundation offering accelerated delivery of innovative applications and unmatch operational efficiency, reliability, administration, security, and control.Overflow;2016-09-3.5Buffer overflow in IBMhttp://wwA-IBM-	
foundation offering accelerated delivery of innovative applications and unmatch operational efficiency, reliability, administration, security, and control.Overflow;2016-09-3.5Buffer overflow in IBMhttp://wwA-IBM-	
operational efficiency, reliability, administration, security, and control.Overflow;2016-09-3.5Buffer overflow in IBMhttp://wwA-IBM-	
Overflow; 2016-09- 3.5 Buffer overflow in IBM http://ww A-IBM-	20
Server (WAS) 7.0 before 01.ibm.co 210916	12
7.0.0.43, 8.0 before m/support 7	
8.0.0.13, 8.5 before /docview.	
8.5.5.10, 9.0 before wss?	
9.0.0.1, and Liberty uid=swg2	
before 16.0.0.3, when 1982588	
HttpSessionIdReuse is enabled, allows remote	
authenticated users to	
obtain sensitive	
information via	
CV         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9	
Scale	-10

			unspecifi Referen 0385			6-				
Websphere	Portal		0305							
IBM WebSph		a set c	of softwai	re tools	that e	nable	es c	ompanie	es to b	uild
and manage								,		
Denial of Service	2016-09- 12		IBM Web 6.1.0 thr CF27, 6.1 6.1.5.3 C through 8.0.0 thr CF21, an CF12 allo authentic cause a c by uploa files. <b>Referen</b> 5954	ough 6 1.5 thro F27, 7 7.0.0.2 ough 8 d 8.5.0 ows ren cated u denial o ding te	.1.0.6 ough 0.0 CF30, .0.0.1 before note sers to of servio mporar	ce ſy	w- 01 /do ws uio	tp://ww ibm.co /support ocview. ss? d=swg2 89993	A-IB WEI	
Jwcrypto Pr	roject	Į Į								
<b>Jwcrypto</b> JWCrypto is an implementation of the Javascript Object Signing and Encryp (JOSE) Web Standards as they are being developed in the JOSE IETF Workir and related technology.										
Gain	2016-09-		obtain cleartext data via a h Million Message Attack (MMA).					tps://git b.com/l chset/jw ypto/rele	e   JŴC	
Gain Information	2016-09-01		Keferen 6298	ce: CV	E-2010	<b>D-</b>		es/tag/v 3.2	9	910/17
Kaspersky	01	4.3	0230				0	۷.۷	9	
Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

Safe Brows	er				
		bv fil	tering out malicious links a	nd inappropr	riate content
			ning websites that may try		
			Kaspersky Safe Browser h		
			indows Phone device.		
			Kaspersky Safe Browser		
			iOS before 1.7.0 does not		
			verify X.509 certificates		
			from SSL servers, which	https://sup	
			allows man-in-the-middle	port.kaspe	
			attackers to obtain	rsky.com/v	
			sensitive information via a	ulnerabilit	A-KAS-
			crafted certificate.	y.aspx?	SAFE
Gain	2016-08-		Reference: CVE-2016-	el=12430	-210916/13
Information	2010 00	43	6231	#280716	0
Let's Php!	25			,, 2007 10	
Simple Cha	+				
		imple	Web and MySQL based cha	t system It a	enerator
			a chat box and a form inpu		
					ew chat line
entries using	AJAX to avo			1	1
			Cross-site scripting (XSS)		
			vulnerability in Let's PHP!		
			simple chat before 2016-		
			08-15 allows remote		
			attackers to inject		
			arbitrary web script or		A 1 FT
			HTML via unspecified		A-LET-
Course alter	2016 00		vectors.		SIMPL-
Cross-site	2016-09-	4.2	Reference: CVE-2016-		210916/13
scripting	01	4.3	4851	NA	1
Mac-telnet					
Mac-telnet					
			and server for connecting to	o Mikrotik Ro	uterOS
routers and l			a MAC address.	-	
Execute	2016-08-	7.5	Buffer overflow in the	https://git	A-MAC-
Code;	30		handle_packet function in	hub.com/h	MAC-T-
Overflow			mactelnet.c in the client	aakonness	210916/13
			in MAC-Telnet 0.4.3 and	joen/MAC-	2
			earlier allows remote	Telnet/pull	
			TELNET servers to	/20	
			execute arbitrary code via		
			a long string in an		
			MT_CPTYPE_PASSSALT		
			control packet.		
CV					
Scoring	0-1 1-2	2-3	3-4 4-5 5-6 6	-7 7-8	8-9 9-10
Scale					

			Reference: CVE-2016- 7115								
Microsoft				<u> </u>							
company's	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	2016-09-	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. <b>Reference: CVE-2016</b> -	http://tech net.micros oft.com/en - us/securit y/bulletin/	A-MIC- EDGE- 210916/13						
Corruption Denial of Service; Execute Code; Overflow; Memory Corruption Denial of Service; Execute Code; Overflow; Memory	14 2016-09- 14 2016-09- 14	7.6 7.6 7.6	3377 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. <b>Reference: CVE-2016- 3350</b> Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-105 http://tech net.micros oft.com/en - us/securit y/bulletin/	3 A-MIC- EDGE- 210916/13 4 A-MIC- EDGE- 210916/13 5						
Corruption	0-1 1-2	2-3	"Microsoft Edge Memory Corruption Vulnerability,"	ms16-105	8-9 9-10						

			a different vulnerability than CVE-2016-3294. <b>Reference: CVE-2016-</b> 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. <b>Reference: CVE-2016-</b> <b>3294</b>	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-105	A-MIC- EDGE- 210916/13 6				
Edge; Inter	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.

MICROSOTT WI	naows line of	oper	ating systems, starting in 19	95.	
			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		A-MIC-
			Disclosure Vulnerability."		EDGE-
Gain	2016-09-		Reference: CVE-2016-		210916/13
Information	14	2.6	3351	NA	7
			Microsoft Internet		
			Explorer 11 and Microsoft		
			Edge allow remote		
			attackers to obtain		
			sensitive information via a		
			crafted web site, aka		
			"Microsoft Browser		
			Information Disclosure		A-MIC-
			Vulnerability."		EDGE-
Gain	2016-09-		Reference: CVE-2016-		210916/13
Information	14	2.6	3325	NA	8

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

	0-1 1-2	2-3		7 7-8	8-9 9-10
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- 210916/14 2
Gain Information	2016-09- 14	2.6		NA	A-MIC- EDGE- 210916/14 1
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." <b>Reference: CVE-2016- 3295</b>	NA	A-MIC- EDGE- 210916/14 0
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." <b>Reference: CVE-2016-</b> <b>3297</b>	NA	A-MIC- EDGE- 210916/13 9

Corruption			corrupti web site Browser Corrupti <b>Refere</b> <b>3247</b>	e, aka "N Memor on Vuln	1icroso <sup>.</sup> y erabilit	ft y."				
Excel										
Microsoft Exc Android and		dshee	t develo	ped by	Microso	oft for	Wir	ndows,	Mac O	S X,
Denial of Service; Overflow Memory Corruption	2016-09- 14		Microso allows r to exect via a cra aka "Mia Memory Vulneral <b>Refere</b> <b>3361</b>	emote a ute arbit afted do crosoft ( Corrup pility."	ittacker rary co cumen Office tion	rs ode t,	net oft. - us/s y/bi	o://tech .micros com/er securit ulletin/ 16-107	A-M EXC	
Excel; Exce				Office	Compa	atibil	ity	Pack; (	Office	Online
<b>Server; Sharepoint Designer</b> 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		Microso Excel 20 2013 SF SP1, Exc 2016 fo Compat Excel Vi Services Server 2 Server 2 Server 2 Automa SharePo SP1, and Server a attacker arbitrary crafted "Microso Corrupti <b>Refere</b>	10 SP2 1, Exce cel 2016 Mac, C ibility Pa ewer, E on Sha 2007 SP on Sha 2010 SP tion Served office allow report s to exce y code v docume oft Office on Vuln	, Excel l 2013 5, Excel office ack SP3 xcel rePoint 3, Exce rePoint 2, Exce vices o rer 201 Online note ecute via a nt, aka e Memo	RT 8, 1 1 1 1 3 5 7 7 9 7 9 7	net oft. - us/s y/b	o://tech .micros com/er securit ulletin/ 16-107	EXC	

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

Service; Overflow Memory2016-09- 14a different vulnerability than CVE-2016-3363. Reference: CVE-2016- 3381- us/securit y/bulletin/ ms16-107A-MIC- EXCEL- 210916/14Corruption149.33381-us/securit us/securit y/bulletin/ ms16-107EXCEL- 210916/14Denial of Service; Overflow Memory2016-09- 14-A-MIC- execute 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-MIC- eXCEL- 2016-09- 2016-09- 4Denial of Service; Overflow Denial of Service; Overflow2016-09- 14A 9.3A-MIC- secel 2010 SP2, Office Compatibility Pack SP3, a different vulnerability + -A-MIC- eXCEL- 210916/14Denial of Service; Overflow2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3,http://tech net.micros oft.com/enDenial of Service; Overflow2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3,http://tech net.micros oft.com/en						
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 PowerPointMicrosoft Excel 2013 SP1, Excel 2013 SP1, Excel 2013 SP1, Excel 2013, 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- 30381http://tech net.micros oft.com/en sybuiltein/ 210916/14 ms16-107Denial of Service; Overflow Denial of Service; Overflow Denial of Service; Overflow Denial of Service; Denial of Service; Denial of Service; Denial of Service; Denial of Service; Denial of Service; Denial of Service; Denial of Service; Denial of Service; 2016-09- Denial of Service; Denial of Service; Denial of Service; 2016-09- Service; 2016-09- Service; Service; 2016-09- Service; 						
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         mewer versions of Word, Excel, and PowerPoint         Microsoft Excel 2010 SP2, Excel 2013 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." a different vulnerability. Service; Overflow       http://tech net.micros oft.com/en net.micros oft.com/en state 2010 SP2, Excel 2013 SP1, Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2010, 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." a different vulnerability and Excel 2013 SP1, Excel 2013 RT SP1, Excel 2010, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption 14 9.3 3363       http://tech A-MIC-         Denial of Service; Ore       2016-09-       SMicrosoft Excel 2007 SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." a different vulnerability." a different vulnerability.       -       A-MIC-         Denial of Service; Over 14       9.3 3363       -       -       -       -       -       -       -					the importa	at document
Office 2003), you will be able to open, edit, and save files using the file formats in newer versions of Word, Excel, and PowerPointmicrosoft Excel 2010 SP2, Excel 2013 SP1, 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- Microsoft Excel 2013 SP1, Excel 2013 RT Service; Overflow Denial of Service; Denial of Service; CorruptionMicrosoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2013 RT SP2, Excel SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a different vulnerability, " a different vu						
Denial of Service; Overflow Memory2016-09- 2016-09- 2016-09- Denial of Service; Denial of Service; Denial of Service; Denial of Service; 2016-09-Microsoft Excel 2007 SP3, Excel 2010, Office Corruption Vulnerability, than CVE-2016-3381. SP1, Excel 2013 SP1, Excel 2013 RT synand Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka mitrosoft Office Memory Corruption Vulnerability, than CVE-2016-3363. SP1, Excel 2010 SP2, Excel 2013 SP1, Excel 2017 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT 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.A-MIC- A-MIC- us/securit y/bulletin/ Service; Denial of Service; 2016-09- Service; 2016-09- CorruptionA-MIC- EXCEL 2013 SP1, Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via y/bulletin/A-MIC- A-MIC- A-MIC- totom/en totom/en totom/en totom/en totom/en totom/en transfer <t< td=""><td>Office 2003)</td><td>, you will be</td><td>able</td><td>to open, edit, and save files</td><td></td><td></td></t<>	Office 2003)	, you will be	able	to open, edit, and save files		
Denial of Service; Overflow MemoryZ016-09- 101-01Excel 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," a different vulnerability," a different vulnerability  Service; Dotenial of Service; Overflow Memory 2016-09-A-MIC- EXCEL- 210916/14 ms16-107Denial of Service; Overflow Memory Denial of Service; Overflow Memory 2016-09-Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, 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," a dif	newer versio	ons of Word, I	Excel,			
Denial of Service; Overflow Denial of Service; Overflow Memory 2016-09- Service; Overflow Memory Service; Overflow Memory Corruption2016-09- Service; Service; Overflow Memory 2016-09- Service; Denial of Service; Overflow Memory 2016-09- Service; Overflow Memory Corruption2016-09- Service; Service; Overflow Memory 2016-09- Service; Denial of Service; Overflow Memory Corruption2016-09- Service; Service; Denial of Service; Service; Denial of Service; Corruption Vallerability, Service; Denial of Service; Service; Service; Denial of Service; <br< td=""><td></td><td></td><td></td><td></td><td></td><td></td></br<>						
Denial of Service; Overflow Denial ofCompatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory different vulnerability," a different vulnerability than CVE-2016-3363.http://tech net.micros oft.com/en - A-MIC- EXCEL- Us/securit 2016-09- CorruptionA-MIC- EXCEL- 2016/14 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 Denial of Service; OverflowA-MIC- 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-MIC- Usersoft Office Memory Corruption Vulnerability. " A-MIC- Excel 2016, Office Compatibility Pack SP3, a different vulnerability." a different vulnerability. " A-MIC- execute arbitrary code via a crafted document, aka ms16-107A-MIC- et.micros oft.com/en oft.com/en oft.com/en oft.com/enDenial of Service; Overflow Memory Corruption2016-09- 9.3Sa63http://tech ms16-107A-MIC- et.micros oft.com/en oft.com/en oft.com/enDenial of Service; Oureflow Memory Corruption2016-09- 9.3Sa63ms16-1076Denial of Service; Compatibility Pack SP3, and Excel Viewer allow remote attackers to weremote attackers to weremote attackers to weremote attackers to weremote attackers to wer				2013 SP1, Excel 2013 RT		
Denial of Service; Overflow Memory2016-09- 9.3and 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. when CVE-2016-3363. when CVE-2016-3363. when CVE-2016-3363. when CVE-2016-3363. when CVE-2016-3363. ms16-107http://tech net.micros oft.com/en 21091614 21091614Denial of Corruption9.33381						
Denial of Service; Overflow2016-09- 9.3remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory than CVE-2016-3363. Reference: CVE-2016- 3381http://tech net.micros oft.com/en us/securitA-MIC- EXCEL- y/bulletin/ 210916/14 ms16-107Denial of Service; Overflow2016-09- 14Reference: CVE-2016- 3381-A-MIC- us/securitMemory Corruption2016-09- 14Reference: CVE-2016- 3381-A-MIC- us/securitDenial of Service; Overflow2016-09- 14Reference: CVE-2016- 3381Denial of Service; Overflow-A-MIC- us/securit-Denial of Service; OverflowDenial of Service; Overflow2016-09- 14Denial of Service; Overflow2016-09- 14-A-MIC- us/securit a different vulnerability." a different vulnerability. -A-MIC- EXCEL- verflow ms16-107Denial of Service; Overflow2016-09- 9.39.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a different vulnerability." a different vulnerability. -A-MIC- EXCEL- 2016-104 ms16-107Denial of Service; Overflow2016-09- 9.39.3Micros						
Denial of Service; Overflow Memory2016-09- 14a crafted document, aka "Microsoft Office Memory Corruption Vulnerability" a different vulnerability than CVE-2016-3363.http://tech net.micros oft.com/en - y/bulletin/ sybulletin/ Sybulletin/ 5Denial of Corruption2016-09- 14Reference: CVE-2016- 3381A-MIC- us/securit y/bulletin/ spb. 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. y/bulletin/http://tech net.micros oft.com/en - A-MIC- us/securit y/bulletin/Denial of Service; Overflow Memory Corruption2016-09- 149.3Microsoft Excel 2007 SP3, excel 2016-3381. Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a dExcel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a dExcel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via and Excel Viewer allow remote attackers to execute arbitrary code via and Excel Viewer allow remote attackers to ybulletin/A-MIC- A-MIC- A-MIC- 210916/14 7				remote attackers to		
Denial of Service; Overflow Memory2016-09- 14"Microsoft Office Memory Corruption Vulnerability than CVE-2016-3363. <b>Reference: CVE-2016-</b> 3381net.micros oft.com/en - us/securit y/bulletin/ ms16-107A-MIC- US 2019/14Denial of Service; Overflow Memory2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT 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 14http://tech net.micros oft.com/en -Denial of Service; Overflow Memory Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016 office Compatibility Pack SP3, a different vulnerability than CVE-2016-3381.http://tech net.micros oft.com/en -Denial of Service; Overflow Memory Corruption2016-09- 9.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a different vulnerability A-MIC- EXCEL-Denial of Service; Overflow Memory Corruption2016-09- 9.39.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via y/bulletin/-A-MIC- 210916/1402016-09- 9.39.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote				-	http://toch	
Denial of Service; Overflow Memory2016-09- 14Corruption Vulnerability, a different vulnerability than CVE-2016-3363. <b>Reference: CVE-2016-</b> <b>3381</b> oft.com/en - us/securit y/bulletin/ 210916/14 ms16-107Corruption149.3 <b>3381</b> -A-MIC- us/securit y/bulletin/ 210916/14 ms16-107Corruption149.3 <b>3381</b> -adifference: CVE-2016- 3381Denial of Service; Overflow Memory2016-09- 16Fixed 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," than CVE-2016-3381.http://tech net.micros oft.com/en oft.com/enDenial of Service; Overflow Memory Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, a different vulnerability, than CVE-2016-3381.http://tech net.micros oft.com/en oft.com/enDenial of Service; Overflow Memory Corruption2016-09- 9.39.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via and Excel Viewer allow remote attackers to execute arbitrary code via-7Corruption149.333637Corruption149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code						
Overflow Memory Corruption2016-09- 14than CVE-2016-3363. Reference: CVE-2016- 3381us/securit y/bulletin/ ms16-107EXCEL- 210916/14Corruption9.3381Wicrosoft 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.http://tech net.micros oft.com/en -A-MIC- EXCEL-Denial of Service; Overflow Memory Corruption2016-09- 149.3Microsoft Excel 2007 SP3, BAG3A-MIC- EXCEL-Denial of Service; Overflow Memory Corruption2016-09- 149.3Microsoft Excel 2007 SP3, BAG3A-MIC- ms16-107Denial of Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via and Excel Viewer allow remote attackers to execute arbitrary code via ybulletin/A-MIC- 7	Denial of			Corruption Vulnerability,"		
Memory Corruption2016-09- 14Reference: CVE-2016- 3381y/bulletin/ ms16-107210916/14Corruption9.33381microsoft 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," a different vulnerability," a different vulnerability," a different vulnerability, a different vulnerability than CVE-2016-3381.http://tech net.micros oft.com/en - A-MIC- EXCEL- 210916/14Denial of Service; Overflow Denial of Service; Overflow Memory Corruption9.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Corruption SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a different vulnerability y/bulletin/A-MIC- EXCEL- 210916/14 7	•				-	
Corruption149.33381ms16-1075Corruption149.33381ms16-1075Microsoft Excel 2007 SP3, 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 Orruption Vulnerability," a different vulnerability than CVE-2016-3381.http://tech net.micros oft.com/en system A-MIC-Denial of Service; Overflow Memory Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Bidference: CVE-2016- Service; Overflow Microsoft Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a difference: CVE-2016- ybulletin/ 210916/14A-MIC- EXCEL- 210916/14Denial of Service; Overflow Memory Corruption2016-09- 9.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via ybulletin/A-MIC- 7		2016-09-				
Denial of Service; Overflow Memory Corruption2016-09- 149.3Excel 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.http://tech net.micros oft.com/en 2016-09- Service; A-MIC- EXCEL- Memory Service;A-MIC- EXCEL- y/bulletin/ 210916/14 GorruptionDenial of Service; Overflow Memory Corruption2016-09- 9.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via y/bulletin/A-MIC- EXCEL- 210916/14 7	Corruption	14	9.3			5
Denial of Service; Overflow Memory Corruption2016-09- 142013 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.http://tech net.micros oft.com/en ybulletin/ 210916/14 CorruptionDenial of Service; Overflow Memory Corruption2016-09- 149.3363-A-MIC- EXCEL- 210916/14 6Denial of Service; Overflow Memory Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code viaA-MIC- EXCEL- 210916/14Overflow Memory Corruption9.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code viaA-MIC- FXCEL- 210916/14						
Denial of Service; Overflow2016-09- 14Reference: CVE-2016-3381. 3363http://tech net.micros oft.com/en oft.com/enDenial of Service; Overflow2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Ompatibility Pack SP3, oft.com/enhttp://tech net.micros oft.com/enDenial of Service; Overflow2016-09- 148.3Reference: CVE-2016- 3381.Juletin/ 210916/14Denial of Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Ompatibility Pack SP3, oft.com/enhttp://tech A-MIC- 210916/14Denial of Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Ompatibility Pack SP3, oft.com/enhttp://tech A-MIC- 7						
Denial of Service; Overflow Ential of Service;2016-09- 14a different vulnerability, a different vulnerability, than CVE-2016-3381.http://tech net.micros oft.com/en - y/bulletin/A-MIC- EXCEL- 2016/04Denial of Service; Overflow Memory Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Office And Excel Viewer allow remote attackers to execute arbitrary code via oft.com/enA-MIC- EXCEL- 2016/14Denial of Service; Overflow Memory Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Office Compatibility Pack SP3, oft.com/enhttp://tech 210916/14 7						
Denial of Service; Overflow2016-09- 149.3remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory corruption Vulnerability," a different vulnerability than CVE-2016-3381.http://tech net.micros oft.com/en - us/securitA-MIC- EXCEL- 210916/14Denial of Service; Overflow Memory Corruption2016-09- 149.3 <b>Reference: CVE-2016-</b> 3363us/securit y/bulletin/ 210916/14EXCEL- 210916/14Denial of Service; Overflow Memory Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code viahttp://tech net.microsA-MIC- EXCEL- 210916/14						
Denial of Service; Overflow2016-09- 14a crafted document, aka "Microsoft Office Memory a different vulnerability," a different vulnerability than CVE-2016-3381.http://tech net.micros oft.com/en - y/bulletin/ 210916/14Denial of Corruption2016-09- 14 <b>Reference: CVE-2016-</b> <b>3363</b> us/securit y/bulletin/ 210916/14Denial of Service; Overflow2016-09- 149.3 <b>Microsoft Excel 2007 SP3,</b> Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code viahttp://tech net.micros oft.com/en 210916/14				remote attackers to		
Denial of Service; Overflow2016-09- 14"Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3381.net.micros oft.com/en - us/securitA-MIC- EXCEL- Us/securitMemory Corruption2016-09- 14 <b>Reference: CVE-2016-</b> <b>3363</b> Nicrosoft Excel 2007 SP3, Excel 2010 SP2, Office Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code viahttp://tech y/bulletin/A-MIC- US/SecuritDenial of Corruption2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code viahttp://tech y/bulletin/A-MIC- US/Securit y/bulletin/					http://toch	
Denial of Service; OverflowCorruption Vulnerability," a different vulnerability than CVE-2016-3381.oft.com/en - us/securitA-MIC- EXCEL- y/bulletin/Memory Corruption2016-09- 149.3Reference: CVE-2016- 3363y/bulletin/ ms16-107210916/14 6Denial of Service; Overflow2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code viahttp://tech y/bulletin/A-MIC- EXCEL-09.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code vianet.micros y/bulletin/EXCEL-					· · .	
Overflow Memory2016-09- 14than CVE-2016-3381.us/securit y/bulletin/ ms16-107EXCEL- 210916/14Corruption149.33363us/securit y/bulletin/ ms16-107EXCEL- 210916/14Denial of Service;2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code viahttp://tech net.microsA-MIC- EXCEL- oft.com/enOverflow Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption44444Memory Corruption4444 </td <td>Denial of</td> <td></td> <td></td> <td>Corruption Vulnerability,"</td> <td></td> <td></td>	Denial of			Corruption Vulnerability,"		
Memory Corruption2016-09- 14Reference: CVE-2016- 3363y/bulletin/ ms16-107210916/14Denial of Service;2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code viahttp://tech net.microsA-MIC- EXCEL- Office oft.com/enMemory Corruption14A-MIC- Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via-	•			, , , , , , , , , , , , , , , , , , ,	- IIS/SACUTIT	
Denial of Service;2016-09- 149.3Microsoft Excel 2007 SP3, Excel 2010 SP2, Office 	Memory	2016-09-			-	-
Service;14Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code vianet.micros oft.com/en 210916/14 7EXCEL- 210916/14 7	Corruption					
Overflow Memory CorruptionCompatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code viaoft.com/en 210916/14 7 us/securit y/bulletin/			9.3		•	
Corruption remote attackers to us/securit execute arbitrary code via y/bulletin/	Overflow	<b>_</b>		Compatibility Pack SP3,		210916/14
execute arbitrary code via y/bulletin/	Memory					7
	Contuption				-	
				-	-	
	CV	0-1 1-2	2-2	3-4 4-5 5-6 6	7 7.8	8-9 9-10
Scoring	Scoring Scale	1-2	2-3	5-4 4-5 5-6 6-	/ /-0	5-5 5-10

			"Microsoft Office Memory Corruption Vulnerability." <b>Reference: CVE-2016-</b>						
			3359						
Excel: Exce	l Viewer: Of	fice	Compatibility Pack; Office	online Ser	ver:				
Sharepoint									
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									
			to open, edit, and save files						
newer versio	ons of Word,	Exce	l, and PowerPoint; SharePoint	nt Designer i	s the tool of				
choice for th	e rapid devel	lopme	ent of SharePoint application	IS.					
			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	http://tech					
			"Microsoft Office Memory	net.micros					
Denial of			Corruption Vulnerability,"	oft.com/en					
Service;			a different vulnerability	-	A-MIC-				
Overflow			than CVE-2016-3362.	us/securit	EXCEL-				
Memory	2016-09-		Reference: CVE-2016-	y/bulletin/	210916/14				
Corruption         14         9.3         3365         ms16-107         8									
		tice	Compatibility Pack; Office	e Online Ser	ver;				
Sharepoint			to Missesoft Office 2000		05-2002				
			to Microsoft Office 2000, (						
			lit, and save files using the RewarRaint ShareRaint Desired						
versions of v	voru, excel,	anu F	PowerPoint .SharePoint Desig	gher is the to	of of choice				

for the rapid development of SharePoint applications.

oring 0-1 1-2 ale	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10
----------------------	---------	---------	-----	-----	-----	------

Denial of Service; Overflow Memory Corruption <b>Exchange S</b> <i>Microsoft Exc</i> <i>Microsoft.</i>	9.3 er is a	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. <b>Reference: CVE-2016- 3362</b>	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-107	A-MIC- EXCEL- 210916/14 9
		Cross-site scripting (XSS) vulnerability in Microsoft Exchange Server 2016 Cumulative Update 1 and 2 allows remote attackers to inject arbitrary web		

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." <b>Reference: CVE-2016-</b> 3379	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-108	A-MIC- EXCHA- 210916/15 0
NA	2016-09- 14	5.8	Open redirect vulnerability in Microsoft Exchange Server 2013 SP1, 2013 Cumulative Update 12, 2013	http://tech net.micros oft.com/en - us/securit	A-MIC- EXCHA- 210916/15 1

CV Scoring Scale	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." <b>Reference: CVE-2016- 3378</b>	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." <b>Reference: CVE-2016- 0138</b>	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-108	A-MIC- EXCHA- 210916/15 2
Internet Exp		<i></i>	nued series of graphical wel		

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.

	2010 00	<b>F</b> 1	Mississ of the trade state		
Bypass	2016-09-	5.1	Microsoft Internet	http://tech	A-MIC-
	14		Explorer 9 through 11	net.micros	INTER-
			mishandles .url files from	oft.com/en	210916/15
			the Internet zone, which	-	3
			allows remote attackers	us/securit	
			to bypass intended access	y/bulletin/	
			restrictions via a crafted	ms16-104	
			file, aka "Internet Explorer		

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

Г	1			1	1
			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." <b>CVE-2016-3324</b> Microsoft Internet Explorer 10 and 11 mishandles integrity settings and zone settings, which allows remote attackers to bypass a sandbox	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-104	A-MIC- INTER- 210916/15 4
			protection mechanism via a crafted web site, aka	http://tech net.micros	
			"Internet Explorer Elevation of Privilege Vulnerability."	oft.com/en - us/securit	A-MIC- INTER-
Bypass	2016-09- 14	5.1	Reference: CVE-2016- 3292	y/bulletin/ ms16-104	210916/15 5
Office	14	J.1	5252	111510-104	5
			te of applications, servers, a	nd services	developed
Gain	2016-09-	4.3	The Visual Basic macros	http://tech	A-MIC-
Information	14		in Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, and 2016 export a	net.micros oft.com/en	OFFIC- 210916/15 6
			certificate-store private	us/securit	Ŭ
			key during a document-	y/bulletin/	
			save operation, which	ms16-107	
			allows attackers to obtain		
			sensitive information via		
			unspecified vectors, aka		
			"Microsoft Information		
			Disclosure Vulnerability." Reference: CVE-2016-		
			RETERETCE: CVE-2010-		
CV		• •			
Scoring	0-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10
Scale					

			0141		
Powerpoint Compatibilit	<b>t; Powerpoi</b> y Pack in ad	<mark>nt Fo</mark> dition	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 Office Web Apps; Office W Mac; Powerpoint Viewe to Microsoft Office 2000, C	<b>r; Sharepo</b> i Office XP, or	7 erver; nt Designer Office 2003,
versions of I	Word, Excel,	and F	lit, and save files using th PowerPoint; SharePoint Desig SharePoint applications.; Po	gner is the t	ool of choice
Denial of Service; Overflow Memory Corruption Office; Office Word For M When used versions of Web App; S	<b>lac; Word V</b> with SharePo Word Web A harePoint De	<b>s; Off</b> <b>iewe</b> oint 20 opp, E signe	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." <b>Reference: CVE-2016- 3360</b> <b>fice Web Apps Server; Sh</b> <i>State State Server</i> <i>Soft Office Web</i> <i>Apps Office Web</i> <i>Apps PowerPoint</i> <i>r is the tool of choice for the</i> <i>for MAC and Word Viewer and</i>	b Apps prov Web App, a he rapid dev	ides updated and OneNote velopment of
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-	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." <b>Reference: CVE-2016- 3357</b>	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-107	A-MIC- OFFIC- 210916/15 9
Outlook; Ou			l information manager from	Microsoft av	ailable as a
part of the M	licrosoft Offic		te.	1	
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." <b>Reference: CVE-2016-</b>	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-107	A-MIC- OUTLO- 210916/16 0

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					
		an ap	oplication framework for w	riting and	running rich
Internet app	lications.			1	1
			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	http://tech	
			crafted web site, aka	net.micros	
Denial of			"Microsoft Silverlight	oft.com/en	
Service;			Memory Corruption	-	A-MIC-
Overflow			Vulnerability."	us/securit	SILVE-
Memory	2016-09-		Reference: CVE-2016-	y/bulletin/	210916/16
Corruption	14	9.3	3367	ms16-109	1
Visio Microsoft Vis	ia ia a dia ara	mmir	a and vactor graphics appli	cation and is	part of the
Microsoft Off			ng and vector graphics appli	Callon and IS	part of the
	ice ranny.		Microsoft Visio 2016		
			allows remote attackers		
			to execute arbitrary code	http://tech	
			via a crafted document,	net.micros	
Denial of			aka "Microsoft Office	oft.com/en	
Service;			Memory Corruption	-	A-MIC-
Overflow			Vulnerability."	us/securit	VISIO-
Memory	2016-09-	0.2	Reference: CVE-2016-	y/bulletin/	210916/16
Corruption	14	9.3	3364	ms16-107	2
MISP-proje	ct formation S	harir	a Platform		
			latform (MISP) allows organi	zations to sh	are
			d their indicators.	200015 00 311	
NA	2016-09-		Malware Information	https://ww	A-MIS-
	03		Sharing Platform (MISP)	w.circl.lu/a	MALWA-
			before 2.3.90 allows	dvisory/CV	210916/16
			remote attackers to	E-2015-	3
			conduct PHP object	5721/	
			injection attacks via		
			crafted serialized data,		
CV					
Scoring	0-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 <b>9-10</b>
Scale					

			attackers to	execute	(	CSA-16-		
Code; SQL Injection	2210 00	,10	SQL injection vulnerabilityhttps://ics- https://ics- velnerabilityA-NAV- WEBAC- 					AC-
<b>Webaccess</b> 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.								
Navis					1	-		
Cross-site scripting NA Navis	2016-09- 03 2016-09- 03		involving (1 edit.ctp, and ajaxification <b>Reference</b> <b>5720</b> app/Control ontroller.ph Information Platform (M 2.3.92 does restrict filen the tmp/file which has u impact and vectors. <b>Reference</b> <b>5719</b>	d (3) i.js. <b>CVE-2015</b> er/Template o in Malwar Sharing SP) before not proper ames unde s/ directory nspecified attack	s- esC e ly r , f- E	https://ww w.circl.lu/a dvisory/CV 2-2015- 5720/ 5720/ https://ww w.circl.lu/a dvisory/CV 2-2015- 5719/	4 A-MI MAL	WA- 916/16
			related to TemplatesC and populate_ev plate_attrib <b>Reference</b> <b>5721</b> Multiple cro scripting (X vulnerabiliti template-cr in Malware Sharing Plat before 2.3.9 remote atta arbitrary we HTML via ve	ent_from_t tes.ctp. <b>CVE-2015</b> ss-site 55) es in the eation featu nformation form (MISP 0 allow ckers to inju- b script or ectors	em j- ure ) ect			

l

			arbitrary SQL commands via unspecified vectors. <b>Reference: CVE-2016-</b>						
			5817	231-01					
Netapp									
	<b>Clustered Data Ontap</b> 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. <b>Reference: CVE-2016-</b> <b>3064</b>	http://kb.n etapp.com /support/in dex? page=con tent&id=9 010099	A-NET- CLUST- 210916/16 7				
NetApp On-C		stem N	<b>jer</b> Manager, which provides fas AS data storage systems	t, simple cor	nfiguration				
			NetApp OnCommand System Manager 8.3.x before 8.3.2P5 allows remote authenticated users to cause a denial of service via unspecified vectors.	http://kb.n etapp.com /support/in dex? page=con tent&id=9 010100	A-NET- ONCOM-				
Denial of Service	2016-09- 01		Reference: CVE-2016- 5047		210916/16 8				
<b>PHP</b> <b>PHP</b> <i>PHP is a serv</i> <i>interactive V</i>	, .		age and a powerful tool for r	making dynai	mic and				
Denial of Service; Overflow	2016-09-		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/C hangeLog- 7.php	A-PHP-PHP- 210916/16 9				
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. <b>Reference: CVE-2016-</b> <b>7134</b>		
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. <b>Reference: CVE-2016-</b> 7133	http://www .php.net/C hangeLog- 7.php	A-PHP-PHP- 210916/17 0
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. <b>Reference: CVE-2016-</b> 7132	https://git hub.com/p hp/php- src/commi t/a14fdb9 74626254 9bbbb96a bb87338b acd147e1 b?w=1	A-PHP-PHP- 210916/17 1
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://git hub.com/p hp/php- src/commi t/a14fdb9 74626254 9bbbb96a bb87338b	A-PHP-PHP- 210916/17 2
CV Scoring Scale	0-1 1-2	2-3		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. <b>Reference: CVE-2016-</b> <b>7131</b>	acd147e1 b?w=1	
Denial of Service Denial of Service	2016-09- 11 2016-09- 11	5 7.5	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. <b>Reference: CVE-2016- 7130</b> 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://git hub.com/p hp/php- src/commi t/698a691 724c0a94 9295991e 5df091ce1 6f899e02? w=1 https://git hub.com/p hp/php- src/commi t/426aeb2 808955ee 3d3f52e0c fb102834c db836a5? w=1	A-PHP-PHP- 210916/17 3 A-PHP-PHP- 210916/17 4

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

			properly validate the number of colors, which		
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	https://bu gs.php.net /bug.php? id=72697	A-PHP-PHP- 210916/17 7
Denial of Service	2016-09-	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. <b>Reference: CVE-2016-</b> 7127	https://bu gs.php.net /bug.php? id=72730	A-PHP-PHP- 210916/17 6
Gain Information	2016-09-	5	that mishandles a dateTime element in a wddxPacket XML document. <b>Reference: CVE-2016-</b> 7129 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. <b>Reference: CVE-2016-</b> 7128	https://git hub.com/p hp/php- src/commi t/6dbb1ee 46b5f4725 cc6519abf 91e512a2 a10dfed? w=1	A-PHP-PHP- 210916/17 5

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. <b>Reference: CVE-2016-</b> <b>7126</b>		
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. <b>Reference: CVE-2016-</b> 7125	https://bu gs.php.net /bug.php? id=72681	A-PHP-PHP- 210916/17 8
Denial of Service	2016-09-	7.5	ext/standard/var_unseriali zer.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. <b>Reference: CVE-2016-</b> 7124	https://bu gs.php.net /bug.php? id=72663	A-PHP-PHP- 210916/17 9
<b>Python</b> Python is an	easy to lear	יסק ו	verful programming languag	e. It has effic	ient hiah-

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.puthead er 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. <b>Reference: CVE-2016-</b> <b>5699</b>	https://hg. python.or g/cpython/ rev/bf3e1c 9b80e9	A-PYT- PYTHO- 210916/18 0
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. <b>Reference: CVE-2016-</b> 5636	https://hg. python.or g/cpython/ raw- file/v2.7.1 2/Misc/NE WS	A-PYT- PYTHO- 210916/18 1
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." <b>Reference: CVE-2016-</b>	https://hg. python.or g/cpython/ rev/d5901 14c2394	A-PYT- PYTHO- 210916/18 2

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

Boodydock			0772		
Readydesk Readydesk					
ReadyDesk i	s a complete		b based help desk software :		has
powerful fea	<u>tures to mee</u> 2016-08- 26	<u>t the</u> 4.6	demands of businesses of an 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. <b>Reference: CVE-2016-</b> 5683	ny size. http://www .kb.cert.or g/vuls/id/2 94272	A-REA- READY- 210916/18 3
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. <b>Reference: CVE-2016-</b> <b>5050</b>	http://www .kb.cert.or g/vuls/id/2 94272	A-REA- READY- 210916/18 4
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.or g/vuls/id/2 94272	A-REA- READY- 210916/18 5
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. <b>Reference: CVE-2016-</b> <b>5048</b>	http://www .kb.cert.or g/vuls/id/2 94272	A-REA- READY- 210916/18 6
Redhat					
Cloudforms					
			nd flexibility while providing	a unified an	a consistent
set or manag	gement capa	onnie	The web UI in Red Hat		
Execute Code	2016-08- 26	6.5	CloudForms 4.1 allows remote authenticated users to execute arbitrary code via vectors involving "Lack of field filters." <b>Reference: CVE-2016-</b> <b>5383</b>	NA	A-RED- CLOUD- 210916/18 7
(BPM). It ena	ss BPM Suite ables enterpri	ise bu	JBoss platform for Business siness and IT users to docur s 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. <b>Reference: CVE-2016-</b> 7034	https://bu gzilla.redh at.com/sh ow_bug.cg i? id=13733 47	A-RED- JBOSS- 210916/18 8
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. <b>Reference: CVE-2016-</b> <b>7033</b>	https://bu gzilla.redh at.com/sh ow_bug.cg i? id=13733 44	A-RED- JBOSS- 210916/18 9
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. <b>Reference: CVE-2016-</b> 6344	https://bu gzilla.redh at.com/sh ow_bug.cg i? id=13718 07	A-RED- JBOSS- 210916/19 0
	tions Network	k simp	olifies developing, testing, de oplications running on it .	eploying and	monitoring
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. <b>Reference: CVE-2016-</b> 5422	NA	A-RED- JBOSS- 210916/19 1
<b>Resteasy</b> RESTEasy is	a JBoss proje	ect tha	at provides various framewo. Tful 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
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

			RESTEasy enables		
			GZIPInterceptor, which	https://bu	
			allows remote attackers to cause a denial of	gzilla.redh at.com/sh	
			service via unspecified	ow bug.cg	A-RED-
			vectors.	i?	RESTE-
Denial of	2016-09-	_	Reference: CVE-2016-	id=13721	210916/19
Service	07	5	6346 RESTEasy allows remote	20	2
			authenticated users to		
			obtain sensitive	https://bu	
			information by leveraging	gzilla.redh	
			"insufficient use of	at.com/sh	
			random values" in async jobs.	ow_bug.cg i?	A-RED- RESTE-
Gain	2016-09-		Reference: CVE-2016-	id=13721	210916/19
Information	07	4	6345	17	3
Rubyonrail					
Ruby On Rail		irce s	oftware to building web app	lication	
			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	http://webl	
			missing WHERE clauses	og.rubyon	
			via a crafted request, as	rails.org/2	
			demonstrated by certain "[nil]" values, a related	016/8/11/ Rails-5-0-	
			issue to CVE-2012-2660,	0-1-4-2-7-	
			CVE-2012-2694, and CVE-	2-and-3-2-	A-RUB-
			2013-0155.	22-3-have-	RUBY
Dunasa	2016-09-	-	Reference: CVE-2016-	been-	-210916/19
Bypass	07	5	6317	released/	4
Siemens					

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

<b>En100 Ethernet Module Firmware</b> Siemens released firmware updates for EN100 Ethernet module included in											
					100 E	tnern	et	moaule	inciu	aea in	
SIPROTEC 4	and SIPROTE	C Con	The EN1 module Siemens SIPROTE devices attacker authenti administ unspecif during a session.	00 Ethe before 4 SIPRO C Comp allows r allows r s to byp cation a crative a red HTT	4.29 for FEC 4 a pact remote pass and obt access P traffi	and ain via c	.sie on oo en cu	:p://www emens.c n/cert/p l/cert/si nens_se rity_adv ory ssa-			
	2016-09-		Referer	nce: CV	E-201	6-		0413.pc		916/19	
Bypass	05	9	7114				f		5		
Denial of Service	2016-09- 05	7.8	The EN1 module Siemens SIPROTE devices attacker denial of mode tra crafted H Referen 7113	before 4 SIPRO C Comp allows r s to cau f service ansition HTTP pa	4.29 for FEC 4 a pact remote use a e (defec ) via ckets.	nd ct-	.sie om oo em cu iso	p://www emens.co n/cert/p l/cert/si nens_se rity_adv ory_ssa- 0413.pc	A-SI EN1		
	2016-09-		The EN1 module Siemens SIPROTE devices attacker authenti administ unspecif <b>Referer</b>	before 4 SIPRO C Comp allows r s to byp cation a crative a ied HTT	4.29 for FEC 4 a bact remote bass and obt access P traffi	aind ain via c.	.sie on oo en cu iso 63	p://www emens.c n/cert/p l/cert/si nens_se rity_adv vry_ssa- 0413.pc	A-SI EN1 I 210		
Bypass	05	10	7112				f		7		
The Forema	an										
ForemanForeman 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-site2016-08-3.5Cross-site scripting (XSS)											
	2016-08-	5.5						.po.,, cite		· <b>-</b>	
CV Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9	9-10	

scripting	19		vulnerability in app/assets/javascripts/hos t_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. <b>Reference: CVE-2016-</b> 6320	foreman.o rg/security .html#201 6-6320	FOREM- 210916/19 8
Cross-site scripting	2016-08- 19	4.3	Cross-site scripting (XSS) vulnerability in app/helpers/form_helper.r b 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. <b>Reference: CVE-2016-</b> 6319	https://bu gzilla.redh at.com/sh ow_bug.cg i? id=13658 15	A-THE- FOREM- 210916/19 9
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/in terfaces. <b>Reference: CVE-2016-</b> 5390	https://bu gzilla.redh at.com/sh ow_bug.cg i? id=13557 28	A-THE- FOREM- 210916/20 0
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://the foreman.o rg/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
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

CV Scoring	0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8	8-9	9-10
<b>Tryton</b> Tryton is	a three-	tier hig	h-level	general	purpose	e comp	uter	арр	lication	n pla	tfori	m on
Tryton												
Bypass	20	 016-08-  19		<b>4475</b> 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. <b>Reference: CVE-2016-</b> <b>4451</b>					tp://pro ts.thefc nan.org ues/151	j pr A /i F	A-TH FORE 2109	
Bypass	20	016-08-		a hostna <b>Referen</b> <b>4995</b> The (1) (2) Loca in Foren and 1.12 RC3 allo authent bypass location (a) read delete a organiza via unsp <b>Referen</b>	ame. nce: CV Organiz ations AF nan befo 2.x befo w remo icated u organiza restrict l, (b) edi arbitrary ations of pecified	<b>E-201</b> ation an Pls and ore 1.11 re 1.12 te sers to ation an ions an t, or (c)	<b>5-</b> nd UIs 4 .0- nd d	6 htt for rg, .ht	tps://the reman.or /securit cml#20 4475	e A	A-TH ORE 2109	
				which a authent permiss hosts to host cor informa	ning ter llows ren icated u ion to vi obtain nfigurati tion via	nplates mote sers wi ew son sensitiv on	th ne ⁄e					

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.												
top of which	is built an Er	nterpr	· · · · · ·	business soli	ution.							
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. <b>Reference: CVE-2016-</b> 1242	https://bu gs.tryton.o rg/issue58 08	A-TRY- TRYTO- 210916/20 4							
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. <b>Reference: CVE-2016-</b> <b>1241</b>	https://bu gs.tryton.o rg/issue57 95	A-TRY- TRYTO- 210916/20 5							
Ultravnc												
All data for t and server c	<b>Repeater</b> 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											
ΝΑ	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.http://www .kb.cert.or g/vuls/id/BA-ULT- REPEA- 210916Reference: CVE-2016- 5673LUU- A9WQVP210916									
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 le	eading applic	ation	of forum and community pu	lblishing soft	ware.					
Execute Code; SQL Injection	2016-08- 30	7.5	SQL injection vulnerability in forumrunner/includes/mo deration.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. <b>Reference: CVE-2016-</b> 6195	http://www .vbulletin. org/forum/ showthrea d.php? t=322848	A-VBU- VBULL- 210916/20 7					
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 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 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. <b>Reference: CVE-2016- 6483</b>	http://www .vbulletin. com/foru m/forum/v bulletin- announce ments/vbu lletin- announce ments_aa/ 4349551- security- patch- vbulletin- 5-2-0-5-2- 1-5-2-2	A-VBU- VBULL- 210916/20 8					
Vmware										
<b>Identity Manger; Vrealize Automation</b> 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
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

			VMware Identity Manager							
			2.x before 2.7 and							
			vRealize Automation 7.0.x before 7.1 allow local	http://www .vmware.c						
			users to obtain root	om/securit						
			access via unspecified	y/advisori	A-VMW-					
			vectors.	es/VMSA-	IDENT-					
	2016-08-		Reference: CVE-2016-	2016-	210916/20					
NA	30	7.2	5335	0013.html	9					
			VMware vRealize	,,						
			Automation 7.0.x before	http://www						
			7.1 allows remote attackers to execute	.vmware.c om/securit						
			arbitrary code via	y/advisori	A-VMW-					
			unspecified vectors.	es/VMSA-	VREAL-					
Execute	2016-08-		Reference: CVE-2016-	2016-	210916/21					
Code	30	7.5	5336	0013.html	0					
Vrealize Lo										
			eterogeneous and highly sca							
			poards, sophisticated analyti							
extensibility,	providing de	eep op	perational visibility and faste	er troublesho						
			Directory traversal		A-VMW- VREAL-					
			vulnerability in VMware vRealize Log Insight 2.x	http://www	210916/21					
			and 3.x before 3.6.0	.vmware.c	1					
			allows remote attackers	om/securit	-					
			to read arbitrary files via	y/advisori						
			unspecified vectors.	es/VMSA-						
Directory	2016-08-		Reference: CVE-2016-	2016-						
Traversal	30	5	5332	0011.html						
Watchguar										
Rapidstrea	m:NA			I						
			WatchGuard RapidStream		A-WAT-					
			appliances allow local		RAPID-					
			users to gain privileges		210916/21 2					
			and execute arbitrary commands via a crafted		2					
			ifconfig command, aka							
Execute			ESCALATEPLOWMAN.							
Code; Gain	2016-08-		Reference: CVE-2016-							
Info	24	7.2	7089	NA						
Wireshark										
Wireshark										
Wireshark is	a network p	rotoco	ol analyzer for Unix and Wind	dows.						
CV		• •								
Scoring	0-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10					
Scale										

			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-	https://bu	
			after-free and application	gs wiresha	
			crash) via a crafted	rk.org/bug	A-WIR- WIRES-
Denial of	2016-09-		packet. <b>Reference: CVE-2016-</b>	zilla/show_ bug.cgi?	210916/21
Service	09	4.3	7180	id=12782	3
			Stack-based buffer	http:///	
			overflow in epan/dissectors/packet-	https://cod e.wireshar	
			catapult-dct2000.c in the	k.org/revie	
			Catapult DCT2000	w/gitweb?	
			dissector in Wireshark 2.x before 2.0.6 allows	p=wiresha rk.git;a=c	
			remote attackers to cause	ommit;h=	
			a denial of service	3b97fbddc	
Devial of			(application crash) via a	23c06572	A-WIR-
Denial of Service;	2016-09-		crafted packet. Reference: CVE-2016-	7b0147aa b52a27c4	WIRES- 210916/21
Overflow	09	4.3	7179	aadffe7	4
			epan/dissectors/packet-		
			umts_fp.c in the UMTS FP dissector in Wireshark 2.x	https://cod	
			before 2.0.6 does not	e.wireshar	
			ensure that memory is	k.org/revie	
			allocated for certain data	w/gitweb?	
			structures, which allows remote attackers to cause	p=wiresha rk.git;a=c	
			a denial of service (invalid	ommit;h=	
			write access and	315bba7c	
			application crash) via a crafted packet.	645b75af2 4215c630	A-WIR- WIRES-
Denial of	2016-09-		Reference: CVE-2016-	3d187b18	210916/21
Service	09	4.3	7178	8610bba	5
Denial of	2016-09-	4.3	epan/dissectors/packet-	https://cod	A-WIR-
Service; Overflow	09		catapult-dct2000.c in the Catapult DCT2000	e.wireshar k.org/revie	WIRES- 210916/21
					210310/21

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. <b>Reference: CVE-2016-</b> <b>7177</b>	w/gitweb? p=wiresha rk.git;a=c ommit;h= 2e37b271 c473e1cb d01d62eb e1f3b011f c9fe638	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. <b>Reference: CVE-2016-</b> <b>7176</b>	https://cod e.wireshar k.org/revie w/gitweb? p=wiresha rk.git;a=c ommit;h= 6d826199 4bb928b7 e80e3a24 78a3d939 ea1ef373	A-WIR- WIRES- 210916/21 7				
Denial of Service	2016-09- 09		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. <b>Reference: CVE-2016-</b> <b>7175</b>	https://cod e.wireshar k.org/revie w/gitweb? p=wiresha rk.git;a=c ommit;h= 1396f6ad5 55178f6b8 1cc1a65f9 cb37b2d9 9aebf	A-WIR- WIRES- 210916/21 8				
	laboration S laboration S								
the cloud, k Zimbra offe	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				

scripting 29 4.3 5721 sories 9	scripting	2016-08- 29	4.3	vulnerabilities in Zimbra Collaboration before 8.7.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors. <b>Reference: CVE-2016-</b> <b>5721</b>	https://wik i.zimbra.c om/wiki/Zi mbra_Sec urity_Advi sories	A-ZIM- ZIMBR- 210916/21 9
--------------------------------	-----------	----------------	-----	--	---	------------------------------------

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; Bigip 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 solution remote access 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 Denial of	2016-08- 19 2016-08-	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 11.6.1, and 12.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 11.6.1, and 12.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 us/solution negotiations via uspecified vectors. 10/sol101 A-F5/-BIG-I- <b>S736</b> https://sup A-F5/-BIG-I-
Service	26		IP systems 11.2.1 HF11port.f5.co210916/22through HF15, 11.4.1 HF4m/kb/en-1through HF10, 11.5.3us/solutionthrough 11.5.4, 11.6.0s/public/k/HF5 through HF7, and19/sol19712.0.0, when configured84568.htwith a TCP profile, allowmlremote attackers to cause
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. <b>Reference: CVE-2016-</b> <b>5023</b>		
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. <b>Reference: CVE-2016-</b> 1497	https://sup port.f5.co m/kb/en- us/solution s/public/k/ 31/sol319 25518.ht ml	A-F5/-BIG-I- 210916/22 2
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://sup port.f5.co m/kb/en- us/solution s/public/k/ 52/sol526 38558.ht ml	A-F5/-BIG-I- 210916/22 3

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

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	Denial of Service	2016-09-07	7.5	11.5.4 H 11.6.1 H before 1 DNS 12. HF3; BIC Gateway and WO 11.2.1 H BIG-IP G 11.2.1 H 11.4.x, 11.5.4 H before 1 PSM 11. HF16, 1 through Manage Cloud an through	5M, and er 11.2. IF16, 11 11.5.x b IF2, 11.0 IF1, and 2.0.0 H M, and I1.5.x b IF2, 11.0 IF1, and 2.0.0 H X before G-IP Edg y, WebA M 11.2.2 IF16 and ITM 11.2 IF16 and ITM 11.2 IF16, 11 11.5.x b IF2, and IF16, 11 11.5.x b IF2, and IF16, 11 11.5.x b IF2, and ITM 11.2 IF16, 11 11.5.x b IF2, and ITM 11.2 IF16, 11 11.5.x b IF2, and ITM 11.2 IF16, 11 II.5.x b IF2, and II.4.1; r 3.1.1; nd Secu 4.5.0; E	Link x before 1.3.x, before 6.x befo 12.x F3; BIG PEM before 6.x befo 12.x F3; BIG e 12.0.0 e 12.0.0 e 12.0.0 e 12.0.0 e 12.0.0 f3; BIG e 12.0.0 f3; BIG t11.6.x F1; BIG ore 11.2 nd 11.4 Enterp BIG-IQ irity 4.0 BIG-IQ	e ore -IP ore -IP 0; ore 2.1 .0 rise	por m/l us/ s/p 06/	ps://sup t.f5.co <b en-<br="">solution ublic/k/ sol060 217.ht</b>		/-BIG-I- 916/22
CV       0-1       1-2       2-3       3-4       4-5       5-6       6-7       7-8       8-9       9-10         Scale       Scale	Scoring	0-1 1-2	2-3					7	7-8	8-9	9-10

				BIG-IQ C Manage IQ Cloud Orchest iWorkflo Packet F on virtu possibly allow re cause a (Traffic I Microke possibly other im network <b>Refere</b> 5022	ement 5. d and ration 1 bw 2.0.0 Filtering al serve v self IP denial of Manage rnel rest v have u npact via c traffic. <b>nce: CV</b>	0.0; BIC .0.0; ar , when is enab rs and address tackers of servion ment cart) an nspecif a crafte	nd bled ses, to ce d ied sd <b>6-</b>				
Gain Privileges	2016-	08- 19	8.5	The Cor in F5 Bl Analytic GTM, ar 11.x be 11.3.x, 11.4.1 H before 1 before 1 11.4.x b HF10, 1 11.5.4, 11.6.1; PEM 11.	G-IP LTM, s, APM, d Link ( fore 11.2 11.4.x b HF10, 11 L1.5.4, a L1.6.1; E offore 12 1.5.x be and 11.0 BIG-IP A .3.x, 11. HF10, 11 L1.5.4, a L1.6.1; E y, WebA M 11.x f HF16 and J-IP PSM L1.2.1 H and 11.4 HF10 allo authent ith certa ions to g	ASM, Controlle 2.1 HF1 efore 5.x nd 11.6 BIG-IP A 1.4.1 fore 5.x befo FM and 4.x befo 5.x nd 11.6 BIG-IP E ccelera before d 11.3.0 11.x F16, 4.x befo bys icated nin gain	er 6, 5.x AM ore ore 5.x dge itor, 0;	po m/ us, s/p 12	ps://sup rt.f5.co kb/en- /solutior public/k/ /sol124 251.ht	210 5 1	5/-BIG-I- 916/22
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. <b>Reference: CVE-2015-</b> 8022		
Cisco					
Asa;Firepo Software;P	wer Threat ix Firewall	Defen	se Software;Firepower Se se Software/Asa 1000v (	Cloud Firew	all
			erprise-class security capa		
			rm factors;Beat sophisticat		
			ustry's first threat-focused ; Firepower Threat Defense		
			n Snort, an open-source int		
			eXchange) was a popular i		
address tran	slation (NAT)				
			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	http://tool	
			packets, aka Bug ID	s.cisco.co m/security	
			CSCva92151 or	/center/vie	A-CIS-
Execute			EXTRABACON.	wErp.x?	ADAPT-
Code;	2016-08-		Reference: CVE-2016-	alertId=ER	210916/22
Overflow	18		6366	P-56516	6
	ssl;Python;				
			ent Appliance/Openssl/Py		Enterprise
	and a second		Enterprise Web Server; J	boss Web	
	erprise Linu			, ,	
			nagement Appliance (SMA) multiple Cisco email and		
	-		tion Platform (or JBoss		
			sed application server rul		
			g highly-transactional Java a		
CV		2.2		7 7-8	0.0.0.10
Scoring	0-1 1-2	2-3	3-4 4-5 5-6 6-	/ / /-0	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.

Sindi ter, and	пос пехіо	<u>, , , , , , , , , , , , , , , , , , , </u>			
			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.	https://ww w.openssl. org/blog/bl og/2016/0	A-CIS- CONTE-
Gain	2016-08-		Reference: CVE-2016-	8/24/swee	210916/22
Information	31	5	2183	t32/	7
		J	2105		/

## 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.

a group or m	uiviuuais cai	eu tr	ie Deblait Floject.		
			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		
Denial of			possibly execute arbitrary		
Service;			code via a crafted		A-COL-
Execute			network packet.	http://colle	COLLE-
Code;	2016-08-		Reference: CVE-2016-	ctd.org/ne	210916/22
Overflow	19	6.4	6254	ws.shtml	8
Cracklib Pro	oiect/Novel				

V coring cale 0-1 1-2 2	3 3-4 4-5	5-6 6-7	7-8 8-9	9-10
-------------------------------	-----------	---------	---------	------

Cracklib/Le		to de	termine whether they match	h certain sec	uritv-
oriented cha					uncy
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. <b>Reference: CVE-2016-</b> 6318	A-CRA- CRACK- 210916/22 9	
	Project/Deb		•		
Dbd-mysql/	Debian Linu	IX: N			
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. <b>Reference: CVE-2015-</b> 8949	A-DBD- DBD-M- 210916/23 0	
Microsoft				/45	
Windows is a sold by Micro	a metafamily osoft. It consi	of gra ists of <u>Wind</u>	8.1;Windows Rt 8.1;Wind aphical operating systems de several families of operating ows server line of operating 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	eveloped, ma g systems.W	arketed, and
CV Scoring Scale	0-1 1-2	2-3	information via a crafted web site, aka "PDF Library Information Disclosure <b>3-4 4-5 5-6 6</b> -	7 7-8	8-9 9-10

			Vulnerability," a different vulnerability than CVE- 2016-3370. <b>Reference: CVE-2016-</b> 3374		
Gain Information Internet Exp 8.1;Window					
Internet Explo systems deve of operating operating sys	orer is a Wel eloped, mark systems; W stems.	o Brov ceted, indow	wser/ Windows is a metafam and sold by Microsoft. It co vs Server series is Microsoft	ily of graphic onsists of sev t Windows se	al operating eral families erver line of
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- 210916/23 3

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/Nu				-	
	Surveillance				
_	r ReadyNAS f managemer		of SOHO and small busines	s nas syste	ems oπers a
			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		
Execute			authenticated users to execute arbitrary code via the sn parameter to the transfer_license command.	http://www .kb.cert.or	READY-
Code; Overflow	2016-08- 31	9	Reference: CVE-2016- 5680	g/vuls/id/8 56152	210916/23 4
Execute	2016-08-		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. <b>Reference: CVE-2016-</b>	http://www .kb.cert.or	A-NET- READY-
Code	31	9	5679	g/vuls/id/8 56152	210916/23 5
		_	nini 2;Nvrsolo	50152	
The Netgear	r ReadyNAS	line o	of SOHO and small busines	s NAS syste	ems offers a
	f managemer				
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.or g/vuls/id/8 56152	A-NET- READY- 210916/23 6
CV Scoring Scale	0-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10

			NVRsolo 1.0.0 through 3.0.0, NUUO Crystal 2.2.1	56152	9
Execute Code	2016-08- 31	10	handle_daylightsaving.ph p in NUUO NVRmini 2 1.7.5 through 3.0.0, NUUO	http://www .kb.cert.or g/vuls/id/8	A-NET- READY- 210916/23
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. <b>Reference: CVE-2016-</b> 5674	http://www .kb.cert.or g/vuls/id/8 56152	A-NET- READY- 210916/23 8
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. <b>Reference: CVE-2016-</b> <b>5676</b>	http://www .kb.cert.or g/vuls/id/8 56152	A-NET- READY- 210916/23 7
			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 annvr_statusphp request. <b>Reference: CVE-2016-</b> 5677		

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

			through NETGEA Surveilla 1.4.1 all attacker arbitrar NTPServ <b>Refere</b> 5675	R Ready ance 1.1 lows ren rs to exe y PHP co ver para	/NAS 1 thro note ecute ode via meter. (E-2010	the				
			Пd	luwar	2					
	utomation									
	wa;1766-132	awaa;	;1766-l3	32bwa;	1766-l	32bw	laa	;1766-		
132bxb;176										
	utomation c									
	ble logic coi									
	m MicroLogix									
	rovides you							ner 1/0	count	, laster
nigh Speed	Counter/PTO	ana ei	<u>nnancea</u> Rockwe			JIITIE.	S			
			MicroLo 1766-L3	0						
			L32AWA	-						
			1766-L3	-		,				
			L32AWA							
			L32BXB	-		a				
			hardcod			u				
			commu							
			it easier							
			attacker			arv	htt	:ps://ics-		
			firmwar					rt.us-		
			leveragi	•	-	of		rt.gov/a	H-R	DC-
			this con					isories/l	176	
	2016-08-		Refere			6-		A-16-		916/24
NA	23	7.5	5645					4-01	0	
Zmodo										
	v;Zp-ne-14-s									
	bh-13w high		tion wir	eless IP	camer	a pro	vio	les a co	mplet	e. cost-
	etwork video									
	retail busines.									
NA	2016-08-		ZModo 2	ZP-NE14	-S and	ZP-	htt	p://www	/ H-ZI	MO-ZP-
	23		IBH-13V	V device	s have	a		.cert.or		
			hardcod					/uls/id/3		916/24
			which m		•		-	735	1	
			remote	attackei	rs to					
CV										
Scoring	0-1 1-2	2-3	3-4	4-5	5-6	6-7	/	7-8	8-9	9-10
Scale										

			TELNET Refere 5081	access v session nce: CV	/E-2010					
NA	2016-08- 23	5	IBH-13V enforce configu which a attacke associa arbitrar using a value. <b>Refere</b> 5650	ZP-NE14 V device a WPA2 ration se llows re rs to tric tion with y access recogni <b>nce: CV</b>	es do no etting, mote gger n an s point l zed SSI <b>/E-201</b>	by D <b>6-</b>	.kb g/v 017	p://wwv .cert.or uls/id/3 735	IB- 210 2	MO-ZP- 916/24
Application Control Eng Appliance A A5/Ace App Engine Mod Application Cisco Ace Ap	eries Applic Control En gine Appliar A4;Ace 4700 Dication Con dule A3;Ace Control En oplication Con ng and applic	gine A nce A3 ) Serie ntrol I Appli gine I ntrol E	Applian B;Ace 4 es Appl Engine cation Module ngine M	ce A1; 700 Selication Module Contro A5 odule Se	Ace 470 ries Ap Contro A1;Ac I Engin	00 Se oplica ol Eng ce Ap de Mo	erie dio gin plic odu	s Appl n Cont e Appl cation le A4;A a next-g	icatio rol En iance Contro Contro Ce	n Igine ol Ition
Denial of Service	2016-09- 12	7.8	Control through 4700 Ap Engine through remote a denia reload) or (2) T Bug ID 0 <b>Refere</b> 6399	CE30 Ap Engine A5 3.3 oplicatio applianc A5 3.3 attacke l of serv via craft LS packe CSCvb10 nce: CV	Module and AC n Contr ces allow rs to ca ice (dev ced (1) s ets, aka 5317. <b>(E-201</b> )	E rol use vice SSL	s.ci m/s /ce nte oSe dvi co-	p://tool isco.co security nter/co nt/Cisc ecurity sory/cis sa- 160908	A 5 H-C 4-	IS-ACE 916/24
Apple		C	Operat	ing Sy	stem					
Iphone Os iOS (formerl	y iPhone OS) cclusively for			perating	system	i crea	ted	and de	velope	ed by
CV Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	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. <b>Reference: CVE-2016-</b> <b>4654</b>	https://sup port.apple .com/HT20 7026	O-APP- IPHON- 210916/24 4
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. <b>Reference: CVE-2016-</b> <b>4657</b>	https://sup port.apple .com/HT20 7107	O-APP- IPHON- 210916/24 5
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. <b>Reference: CVE-2016-</b> <b>4656</b>	https://sup port.apple .com/HT20 7107	O-APP- IPHON- 210916/24 6
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. <b>Reference: CVE-2016-</b> <b>4655</b>	https://sup port.apple .com/HT20 7107	O-APP- IPHON- 210916/24 7
			cture software, delivering a ss-critical services, and hard		

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 <b>Cisco</b>	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. <b>Reference: CVE-2016-</b> 4376	https://h2 0566.www 2.hpe.com /hpsc/doc/ public/disp lay? docId=em r_na- c0523621 2	O-BRO- FABRI- 210916/24 8				
IOS:NA									
Gain Information	Gain2016-09-The PPTP server in Cisco IOS 15.5(3)M does not properly initialize packet buffers, which allows remote attackers to information from earlier ntent/Cisc oSecurityA dvisory/cis co-sa- 20160902- 210916/24The PPTP server in Cisco IOS 15.5(3)M does not properly initialize packet s.cisco.co m/security /center/co obtain sensitive information from earlier aka Bug ID CSCvb16274. CO-sa- CO-CIS-IOS- 20160902- 210916/24								
<b>los Xr</b> 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 Service2016-08- 22Memory 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.http://tool 									
CV Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10									

				1					
			Cisco IP Phone 8800	http://tool					
			devices with software	s.cisco.co					
			11.0(1) allow remote	m/security					
			attackers to cause a	/center/co					
				ntent/Cisc					
			denial of service (memory						
			corruption) via a crafted	oSecurityA					
Denial of			HTTP request, aka Bug ID	dvisory/cis	O-CIS-IP				
Service;			CSCuz03038.	co-sa-	PH-				
Memory	2016-08-		Reference: CVE-2016-	20160817-	210916/25				
Corruption	22	7.8	1479	ipp	1				
Ip Phone 8	800 Series F	= irmv	vare						
<b>Ip Phone 8800 Series Firmware</b> The Cisco IP Phone 8800 Series delivers HD video and VoIP communications, and									
			vice to meet your business i						
incegraces w		ne de	Cross-site scripting (XSS)	http://tool					
			vulnerability on Cisco IP	s.cisco.co					
			Phone 8800 devices with	m/security					
			software 11.0 allows	/center/co					
			remote authenticated	ntent/Cisc					
			users to inject arbitrary	oSecurityA					
			web script or HTML via	dvisory/cis					
			crafted parameters, aka	co-sa-	O-CIS-IP				
			Bug ID CSCuz03024.	20160810-	PH-				
Cross-site	2016-08-		Reference: CVE-2016-	ip-phone-	210916/25				
scripting	22	3.5	1476	8800	2				
I <sup>-</sup> J									
Spa300 Sei	ries Ip Phon		-						
		e Fir	mware;Spa500 Series Ip	Phone Firm	ware				
Cisco Spa30	0 Series Ip I	<mark>e Fir</mark> Phone	mware;Spa500 Series Ip	Phone Firm al features,	ware such as call				
Cisco Spa30 forwarding,	0 Series Ip I redialing, sp	<mark>e Fir</mark> Phone	mware;Spa500 Series Ip	Phone Firm al features,	ware such as call				
Cisco Spa30	0 Series Ip I redialing, sp	<mark>e Fir</mark> Phone	<b>mware;Spa500 Series Ip</b> Firmware provide tradition dialing, transferring calls,	Phone Firm al features,	ware such as call				
Cisco Spa30 forwarding,	0 Series Ip I redialing, sp	<b>e Fir</b> Phone	<b>mware;Spa500 Series Ip</b> Firmware provide tradition dialing, transferring calls, The HTTP framework on	Phone Firm al features, conference	ware such as call				
Cisco Spa30 forwarding,	0 Series Ip I redialing, sp	<b>e Fir</b> Phone	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, The HTTP framework on Cisco SPA300, SPA500,	Phone Firm pal features, conference http://tool	ware such as call				
Cisco Spa30 forwarding,	0 Series Ip I redialing, sp	<b>e Fir</b> Phone	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, The HTTP framework on Cisco SPA300, SPA500, and SPA51x devices	Phone Firm al features, conference http://tool s.cisco.co	ware such as call				
Cisco Spa30 forwarding,	0 Series Ip I redialing, sp	<b>e Fir</b> Phone	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, The HTTP framework on Cisco SPA300, SPA500, and SPA51x devices allows remote attackers	Phone Firm bal features, conference http://tool s.cisco.co m/security	<b>ware</b> such as call				
Cisco Spa30 forwarding,	0 Series Ip I redialing, sp	<b>e Fir</b> Phone	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, The HTTP framework on Cisco SPA300, SPA500, and SPA51x devices allows remote attackers to cause a denial of	Phone Firm al features, conference http://tool s.cisco.co	ware such as call				
Cisco Spa30 forwarding,	0 Series Ip I redialing, sp	<b>e Fir</b> Phone	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, The HTTP framework on Cisco SPA300, SPA500, and SPA51x devices allows remote attackers	Phone Firm bal features, conference http://tool s.cisco.co m/security	ware such as call				
Cisco Spa30 forwarding,	0 Series Ip I redialing, sp	<b>e Fir</b> Phone	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, The HTTP framework on Cisco SPA300, SPA500, and SPA51x devices allows remote attackers to cause a denial of	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co	ware such as call				
Cisco Spa30 forwarding,	0 Series Ip I redialing, sp	<b>e Fir</b> Phone	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc	ware such as call				
Cisco Spa30 forwarding,	0 Series Ip I redialing, sp	<b>e Fir</b> Phone	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis	ware such as call calling and O-CIS-				
Cisco Spa30 forwarding, accessing vo	0 Series Ip F redialing, sp pice mail.	<b>e Fir</b> Phone	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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.	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa-	ware such as call calling and O-CIS- SPA30-				
Cisco Spa30 forwarding, accessing vo	0 Series Ip F redialing, sp pice mail. 2016-09-	e Fir	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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-	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831-	o-CIS- SPA30- 210916/25				
Cisco Spa30 forwarding, accessing vo Denial of Service	0 Series Ip F redialing, sp pice mail. 2016-09- 11	e Fir Phone beed 7.8	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- spa	O-CIS- SPA30- 210916/25 3				
Cisco Spa30 forwarding, accessing vo Denial of Service <b>Wireless La</b>	0 Series Ip F redialing, sp pice mail. 2016-09- 11 an Controlle	Phone Deed 7.8	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- spa	o-CIS- SPA30- 210916/25 3 <b>are</b>				
Cisco Spa30 forwarding, accessing vo Denial of Service Wireless La 6.0;Wireles	2016-09- 11 <b>an Controlle</b>	7.8 7.8	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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 tware;Wireless Lan Contin Software 7.0;Wireless La	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- spa roller Softw	O-CIS- SPA30- 210916/25 3 are r Software				
Cisco Spa30 forwarding, accessing vo Denial of Service Wireless La 6.0;Wireles 7.1;Wireles	2016-09- 11 <b>an Controlle</b>	7.8 7.8	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- spa roller Softw	O-CIS- SPA30- 210916/25 3 are r Software				
Cisco Spa30 forwarding, accessing vo Denial of Service Wireless La 6.0;Wireles 7.1;Wireles 7.4	2016-09- 11 an Controlle 5 Lan Contro	7.8 7.8 7.8	mware;Spa500 Series Ip I Firmware provide tradition dialing, transferring calls, 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 tware;Wireless Lan Contre Software 7.0;Wireless La	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- spa roller Softw an Controlle	O-CIS- SPA30- 210916/25 3 are r Software r Software				
Cisco Spa30 forwarding, accessing vo Denial of Service Wireless La 6.0;Wireles 7.1;Wireles 7.4	2016-09- 11 an Controlle 5 Lan Contro	7.8 7.8 7.8	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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 tware;Wireless Lan Contin Software 7.0;Wireless La	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- spa roller Softw an Controlle	O-CIS- SPA30- 210916/25 3 are r Software r Software				
Cisco Spa30 forwarding, accessing vo Denial of Service Wireless La 6.0;Wireles 7.1;Wireles 7.4 Cisco Wirel	2016-09- 11 an Controlle 5 Lan Contro	7.8 7.8 7.8	mware;Spa500 Series Ip I Firmware provide tradition dialing, transferring calls, 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 tware;Wireless Lan Contre Software 7.0;Wireless La	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- spa roller Softw an Controlle	O-CIS- SPA30- 210916/25 3 are r Software r Software				
Cisco Spa30 forwarding, accessing vo Denial of Service Wireless La 6.0;Wireles 7.1;Wireles 7.4 Cisco Wirel	2016-09- 11 an Controlle 5 Lan Contro	7.8 7.8 7.8	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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 tware;Wireless Lan Contro Software 7.0;Wireless La Software 7.2;Wireless La	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- spa roller Softw an Controlle	O-CIS- SPA30- 210916/25 3 are r Software r Software				
Cisco Spa30 forwarding, accessing vo Denial of Service Wireless La 6.0;Wireles 7.1;Wireles 7.4 Cisco Wirel	2016-09- 11 an Controlle 55 Lan Contr ess LAN Co	7.8 7.8 7.8 7.8 7.8 7.8 7.8	mware;Spa500 Series Ip Firmware provide tradition dialing, transferring calls, 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 tware;Wireless Lan Contro Software 7.0;Wireless La Software 7.2;Wireless La	Phone Firm al features, conference http://tool s.cisco.co m/security /center/co ntent/Cisc oSecurityA dvisory/cis co-sa- 20160831- spa roller Softw an Controlle	ware such as call calling and O-CIS- SPA30- 210916/25 3 are oftware oftware oftware oftware				

performance of all mobile devices, offers limited hotspot coverage.									
Denial of Service Debian Debian Linu	2016-09- 11	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 request over SNMP, aka Bug ID CSCuz40221.http://tool 							
	g system is		et of basic programs and	utilities that	make your				
compared run.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.http://www openwall. com/lists/o Ss-Denial of Service2016-08- 31Reference: CVE-2016- 31016/08/31 3210916/25Fortinet314.97118/35									
Fortianalyz	Fortianalyzer Firmware;Fortimanager Firmware FortiClient is fully integrated with FortiGate, FortiManager, and FortiAnalyzer for								
CV Scoring Scale	Scoring         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. <b>Reference: CVE-2016-</b> <b>3195</b>	http://forti guard.com /advisory/f ortimanag er-and- fortianalyz er-client- side-xss- vulnerabili ty	O-FOR- FORTI- 210916/25 6				
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. <b>Reference: CVE-2016- 3194</b>	http://forti guard.com /advisory/f ortimanag er-and- fortianalyz er-xss- vulnerabili ty	O-FOR- FORTI- 210916/25 7				
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://forti guard.com /advisory/f ortimanag er-and- fortianalyz er- persistent- xss- vulnerabili ty-1	0-FOR- FORTI- 210916/25 8				

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

vectors. Reference: CVE-2016- 3193Fortios;FortiswitchUse 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.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. FORTI- fortiswitch Portiswitch Data Center ange of models to fit any environment.Execute Code: 2016-08- 092016-08- 10Portiswitch FortiSwitch Data Center ange of models to fit any environment.Bypass2016-09- 090910108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW-244D-POE, FSW-244D-POE, FSW- 224D-POE, FSW- 224D-FPOE, FSW- <br< th=""><th></th><th></th><th></th><th></th><th></th><th></th></br<>											
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.and are available in a wide range of models to fit any environment.Buffer overflow in the Cookie parser in 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- Overflow 2 2016-08- Coverflow 2 2016-08- PortiSwitch Data Center and Secure Access Switches are cost-effective and flexible, and are available in a wide range of models to fit any environment.0-FOR- FOR- FOR- FOR- FOR- FOR- FOR- PortiswitchBypass2016-09- 0910Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW-242D-POE, FSW-248D-FPOE, FSW- 2440D, FSW-448D-POE, FSW-424D-FPOE, FSW- 448D, FSW-448D-POE, FSW-448D-FPOE, FSW- 448D, FSW-448D-POE, FSW-244D-FPOE, FSW- 448D, FSW-448D-FPOE, FSW- 448D, FSW-548D-FPOE, FSW- 448D, FSW-3032D, and FSW-548D, FWS-548D- FPOE, FSW-124D, POE models, when in FortiLink0				Reference: CVE-2016-							
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. Buffer overflow in the Cookie parser in Fortinet FortiOS 4.x before 4.1.11, 4.2.x before 4.3.9 and FortiSwitch before 3.4.3 allows remote attackers to execute arbitrary code via a crafted HTTP request, aka EXECUTE Code; 2016-08- Coverflow 24 10 6909 Fortiswitch Data Center and Secure Access Switches are cost-effective and are available in a wide range of models to fit any environment. Bypass 2016-09- 09 10 Fortiswitch Fortiswitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-FOE, FSW-224D- FPOE, FSW-248D-FPOE, FSW-248D-FPOE, FSW- 448D, FSW-424D-POE, FSW-424D-FPOE, FSW- 448D, FSW-448D-POE, FSW-448D-FPOE, FSW- 448D, FSW-448D-POE, FSW-448D-FPOE, FSW- 448D, FSW-448D-POE, FSW-448D-FPOE, FSW- 224D-FOE, FSW-224D- PFOE, FSW-248D-POE, FSW-448D-FPOE, FSW- 448D, FSW-424D-POE, S24D, FSW-244B-POE, FSW-448D-FPOE, FSW- 448D, FSW-448D-POE, FSW-448D-FPOE, FSW- 448D, FSW-448D-POE, FSW-448D-FPOE, FSW- 448D, FSW-448D-POE, FSW-448D-FPOE, FSW- 448D, FSW-448D-POE, FSW-448D-FPOE, FSW- 448D, FSW-548D, FPOE, FSW-124D, FSW-548D, FSW-548D- FPOE, FSW-124D, FSW-412D-POE, FSW- 448D, FSW-548D, FPOE, FSW-124D, FSW-448D-FPOE, FSW- 448D, FSW-548D, FPOE, FSW-124D, FSW-448D-FPOE, FSW- 524D, FSW-548D, FPOE, FSW-124D, FSW-424D-FPOE, FSW- 524D, FSW-548D, FPOE, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink	Fortios;Fo	rtiswitch									
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.Buffer overflow in the Cookie parser in Fortinet FortiOS 4.x before 4.1.11, 4.2.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. FortiSwitch Data Center and Secure Access Switches are cost-effective 210916/25 023O-FOR- PORTI- 210916/25 023Execute Code; 2016-08- Overflow and are available in a wide range of models to fit any environment.O-FOR- PORTI- 210916/25 023Bypass Dypass2016-09- 10Tortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW-242D- POE, FSW-248D-POE, FSW- 2240-POE, FSW-248D-POE, FSW- 2240-POE, FSW-248D-POE, FSW- 448D, FSW-448D-POE, SPW- 448D, FSW-448D-POE, SPW- 448D, FSW-448D-POE, SPW- 448D, FSW-548D, FSW-548D, FPOE, FSW- 448D, FSW-548D, FSW-548D, FPOE, FSW-<	Use FortiGa	ate to provide	remo	te management for FortiSw	itch units. T	he FortiGate					
and are available in a wide range of models to fit any environment.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 											
Execute Code; Code; 2016-08- DverflowBuffer 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- Overflowhttp://forti guard.com (Advisory/ FORTI- FORTI- 210916/25 023O-FOR- FORTI- FORTI- 210916/25FortiSwitch Data Center and Secure Access Switches are cost-effective and flexible, and are available in a wide range of models to fit any environment.O-FOR- FORTI- FORTI- guard.com (Advisory/ FORTI- 210916/25 023O-FOR- FORTI- FORTI- 210916/25Bypass2016-09- 0910Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW-248D-POE, FSW-248D-FPOE, FSW- 224D-POE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- account- exposed- under- S24D, FSW-424D-POE, FSW-424D-FPOE, FSW- 448D, FSW-448D-POE, FSW-424D-FPOE, FSW- admin- account- exposed- under- specific- ConditionsO-FOR- FORTI- ConditionsFSW-548D, FSW-548D, FFOE, FSW- 1048D, FSW-5102-POE models, when in FortiLinkImage: Specific- conditions	FortiSwitch	Data Center a	and Se	ecure Access Switches are co	ost-effective	and flexible,					
ExecuteCookie parser in Fortinet FortiOS 4.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 Overflowhttp://forti FORTI- 210916/25 023O-FOR- FORTI- 210916/25 023Execute Coverflow241069090239FortiSwitch Data Center and Secure Access Switches are cost-effective and flexible, and are available in a wide range of models to fit any environment.0-FOR- FORTI- 210916/25 0239Bypass2016-09-10FortiSwitch FSW- FSW-124D-POE, FSW- 224D-POE, FSW-248D-POE, FSW-248D-POE, FSW- 244D-FPOE, FSW- 224D-POE, FSW-248D-POE, FSW-248D-POE, FSW- 448D, FSW-448D-POE, FSW-448D-POE, FSW-448D-POE, FSW- 448D, FSW-448D-POE, FSW-448D-POE, Conditions0Forti- FSW-548D, FSW-548D- FOPC, FSW-548D, FSW-548D, FOPC, FSW-548D, FSW-548D, FOPC, FSW-1024D, FSW- 448D, FSW-548D, FSW-548D, FOPC, FSW-1048D, FSW-548D, FOPC, FSW-1048D, FSW-548D, FOPC, FSW-1048D, FSW-548D, FOPC, FSW-1024D, POE, Men in FortiLinkIstension Istension Istension	and are ava	ailable in a wid	<u>le ran</u>	-	ronment.						
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. (advisory/ FORTI- Code; 2016-08- Overflow 24Http://forti guard.com FORTI- Codes 023O-FOR- FORTI- 210916/25 023Fortiswitch 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.Bypass2016-09- 0910Fortinet FortiSwitch FSW- FSW-124D-POE, FSW-124D, FSW-248D-POE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- at24D, FSW-424D-POE, FSW-424D-FOE, FSW- admin- adzisoryf0-FOR- FORTI- 210916/26 0.10916/26 0.10916/26010Fortinet FortiSwitch FSW- FSW-248D-POE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- adcount- exposed- under- S24D, FSW-524D-FPOE, FSW-448D-FPOE, FSW- specific- S24D, FSW-524D-FPOE, FSW-548D, FSW-548D, FSW- S24D, FSW-524D-FPOE, FSW-1048D, FSW-548D, FONE, FSW-1048D, FSW- SW-81048D, FSW-548D, FONE, FSW-1048D, FSW- specific- conditions											
Execute Code; 2016-08- Overflow4.2.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. FORTI- 210916/25 0230-FOR- FORTI- 210916/25 023Execute Code; Overflow241069090-FOR- FORTI- 210916/25 0230-FOR- FORTI- 210916/25 023Fortiswitch Fortiswitch Bypass2016-09-10Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW-242D- POE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- 424D, FSW-248D-FPOE, FSW- account- FSW-248D-FPOE, FSW- admin- 424D, FSW-448D-POE, FSW-448D-FPOE, FSW- admin- 424D, FSW-448D-POE, FSW-448D-FPOE, FSW- account- exposed- under- specific- conditions0Fortiswitch FPOE, FSW-1024D, FSW- FSW-448D-FPOE, FSW- 1048D, FSW-548D, FSW-548D, FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R112D-POE models, when in FortiLink0				•							
Execute Code; Overflow2016-08- 24104.3.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. Gode; Overflowhttp://forti guard.com /advisory/ FORTI- 210916/25 0230-FOR- FORTI- 210916/25 023Fortiswitch Bypass2016-09- 0910Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW-244D-POE, FSW-244D-POE, FSW-244D-POE, FSW-244D-FPOE, FSW-244D-POE, FSW-244D-FPOE, FSW- 424D, FSW-424D-FPOE, FSW- admin- account- FSW-448D-FPOE, FSW- 424D, FSW-448D-FPOE, FSW-448D-FPOE, FSW- 524D, FSW-524D-FPOE, FSW-544D, FSW-544D-FPOE, FSW-448D-FPOE, FSW- 1048D, FSW-544D-FPOE, FSW-544D-FPOE, FSW- 1048D, FSW-544D-FPOE, FSW-544D-FPOE, FSW-544D, FSW-544D-FPOE, FSW-544D, FSW-544D-FPOE, FSW-544D, FSW-544D-FPOE, FSW-544D, FSW-544D-FPOE, FSW-544D, FSW-544D-FPOE, FSW-544D, FSW-544D-FPOE, FSW-544D, FSW-1044BD, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLinkO-FOR- FORTI- 210916/26											
ExecuteFortiSwitch before 3.4.3 allows remote attackers to execute arbitrary code via a crafted HTTP request, akahttp://forti guard.comO-FOR-ExecuteEGREGIOUSBLUNDER. (Advisory/ 24/advisory/ FORTI- 210916/25FORTI- 210916/25Overflow241069090239Fortiswitch FortiswitchFortiswitch Data Center and Secure Access Switches are cost-effective and are available in a wide range of models to fit any environment.Bypass2016-09- 0910Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW-224D- 75W-248D-POE, FSW-248D-POE, FSW-424D-FPOE, FSW- 424D, FSW-424D-FPOE, FSW- 424D, FSW-424D-POE, FSW-424D-FPOE, FSW- 448D, FSW-448D-POE, FSW-448D-FPOE, FSW- 448D, FSW-448D-POE, FSW-548D, FSW-548D, FSW- 524D, FSW-548D, FSW-548D, FSW- 524D, FSW-548D, FSW- 1048D, FSW-1024D, FSW- 1048D, FSW-1024D, FSW- 1048D, FSW-112D-POE models, when in FortiLinko				-							
Execute Code; Overflow2016-08- 24allows remote attackers to execute arbitrary code via a crafted HTTP request, aka EGREGIOUSBLUNDER. (Advisory/ FG-IR-16- 0230-FOR- FORTI- FG-IR-16- 210916/25 023Fortiswitch Fortiswitch Data Center and zer available in a wite and are available in a wite 09Tortiswitch SW: Fortinet FortiSwitch FSW- 10 BOP-POE, FSW-124D, POE, FSW-124D, POE, FSW-24D-POE, FSW- 224D-POE, FSW-224D- 001http://forti guard.com FORTI- guard.com FORTI- 210916/26Bypass2016-09- 0910 Fortinet FortiSwitch FSW- 108D-POE, FSW-224D- FSW-124D-POE, FSW- 224D-POE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- 424D, FSW-424D-POE, FSW-424D-FPOE, FSW- admin- 424D, FSW-424D-FPOE, FSW- admin- 424D, FSW-424D-FPOE, FSW- admin- 424D, FSW-448D-FPOE, FSW-524D, FSW-524D, FSW- specific- 524D, FSW-524D, FSW- 524D, FSW-524D, FSW- 524D, FSW-524D, FSW- 524D, FSW-1024D, FSW- 1048D, FSW-112D-POE models, when in FortiLinkunder- specific- conditions											
Executeto execute arbitrary code via a crafted HTTP request, akahttp://forti guard.com /advisory/O-FOR- FORTI- 210916/25Code;2016-08- 02 24EGREGIOUSBLUNDER. 6909/advisory/FORTI- 210916/25Fortiswitch241069090239Fortiswitch Data Center and Secure Access Switches are cost-effective and flexible, and are available in a wide range of models to fit any environment.Bypass2016-09-10Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- 424D, FSW-424D-POE, FSW- account- FSW-424D-FPOE, FSW- account- FSW-424D-FPOE, FSW- account- FSW-448D-FPOE, FSW- specific- conditionsO-FOR- FORTI- 210916/26Image: text of t											
via a crafted HTTPhttp://fortiExecuteuia a crafted HTTPhttp://fortiExecuteEGREGIOUSBLUNDER./advisory/Code;2016-08-Reference: CVE-2016-Overflow2410FortiswitchFortiswitch Data Center and Secure Access Switches are cost-effective and flexible, and are available in a widerarge of models to fit any environment.Bypass2016-09-10Fortinet FortiSwitch PSW-0.9108D-POE, FSW-124D,guard.comBypass2016-09-10Fortinet FortiSwitch FSW-http://forti00.9108D-POE, FSW-124D,guard.comFORTI-FSW-124D-POE, FSW-/advisory/f210916/26224D-POE, FSW-248D-POE,rest-FSW-248D-FPOE, FSW-admin-424D, FSW-424D-POE,account-FSW-424D-FPOE, FSW-account-FSW-448D-FPOE, FSW-specific-524D, FSW-548D, FSW-548D-conditionsFSW-548D, FSW-548D, FSW-548D-FOE, FSW-1024D, FSW-1048D, FSW-302D, andFSW-7112D-POE models,when in FortiLinkwhen in FortiLink											
Execute Code; Overflow2016-08- 24request, aka EGREGIOUSBLUNDER. Reference: CVE-2016- 023guard.com /advisory/ FG-IR-16- 023O-FOR- FORTI- 210916/25 9Fortiswitch Data Center and Secure Access Switches are cost-effective and are available in a wide range of models to fit any environment.Bypass2016-09-10Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW-248D-POE, FSW-248D-POE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- account- exposed- under- S24D, FSW-544D-FOE, FSW- 448D, FSW-448D-FPOE, FSW- 524D, FSW-544D-FPOE, FSW- specific- conditions0-FOR- FORTI- FORTI- 210916/26 0-FOR- fortiswitch- 0FSW-448D, FSW-448D-FPOE, FSW-448D-FPOE, FSW- 448D, FSW-448D-FPOE, FSW-544D-FPOE, FSW- 524D, FSW-544D-FPOE, Specific- conditions0FSW-548D, FSW-548D- FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink0					http://farti						
Execute Code; Overflow2016-08- 24EGREGIOUSBLUNDER. Reference: CVE-2016- 6909/advisory/ FG-IR-16- 023FORTI- 210916/25 9Fortiswitch Portiswitch Data Center and Secure Access Switches are cost-effective and flexible, and are available in a wide range of models to fit any environment.Bypass2016-09- 0910Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW-244D, FSW-244D-POE, FSW- 224D-POE, FSW-248D-POE, FSW-248D-FPOE, FSW- 424D, FSW-448D-FPOE, FSW-448D-FPOE, FSW- 448D, FSW-448D-FPOE, FSW-448D-FPOE, FSW- 448D, FSW-448D-FPOE, FSW-448D-FPOE, FSW- 524D, FSW-548D, FSW-548D, FSW-548D, FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink/advisory/f FORTI- 210916/26 0O-FOR- FORTI- 210916/26 0											
Code; Overflow2016-08- 24Reference: CVE-2016- 6909FG-IR-16- 023210916/25 9Fortiswitch 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.Bypass2016-09- 0910Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW- 224D-POE, FSW-248D-POE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- 424D, FSW-244D-FPOE, FSW- admin- 424D, FSW-424D-FPOE, FSW- admin- 424D, FSW-448D-FPOE, FSW- specific- conditionsO-FOR- FORTI- 210916/26 0Bypass2016-09- 0910Fortinet FortiSwitch FSW- 108D-POE, FSW- 224D-POE, FSW- 224D-POE, FSW- admin- 424D, FSW-244D-POE, specific- conditionsO-FOR- FORTI- 210916/26 0Bypass2016-09- 0910Fortinet FortiSwitch FSW- 108D-POE, FSW- 224D-POE, FSW- admin- account- FSW-448D-FPOE, FSW- account- FSW-448D-FPOE, FSW- specific- conditionsO-FOR- FOR- FOR- FSW-548D, FSW-548D- FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLinkImage: Display the displ	Execute			•							
Overflow241069090239FortiswitchFortiswitch Data Center and Secure Access Switches are cost-effective and flexible, and are avaible in a wide rarge of models to fit any environment.Bypass2016-09-10Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW- 224D-POE, FSW-248D-POE, FSW-248D-POE, FSW-248D-POE, FSW-248D-FOE, FSW- admin- account- FSW-248D-FPOE, FSW- admin- account- FSW-424D, FSW-424D-POE, FSW-424D-FOE, FSW- admin- account- FSW-448D, FSW-448D-POE, Specific- S24D, FSW-524D-FPOE, Conditions9FSW-548D, FSW-548D, FSW-548D, FSW-548D, FSW-548D, FSW-548D, FPOE, FSW-1024D, FSW-9Intervent Intervent9Overflow Intervent Intervent Intervent Intervent Intervent Intervent Intervent Intervent Intervent Intervent Intervent Intervent Intervent Intervent9Overflow Intervent<		2016-08-									
FortiswitchFortiswitch Data Center and Secure Access Switches are cost-effective and flexible, and are available in a wide range of models to fit any environment.Bypass2016-09-10Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW-224D- 001http://forti guard.com FORTI- 210916/26 0O-FOR- FORTI- 210916/26 0Bypass2016-09-10Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW-224D- 0http://forti guard.com FORTI- 210916/26 0O-FOR- FORTI- 210916/26 0Bypass2016-09-10Fortinet FortiSwitch FSW- (advisory/f 224D-POE, FSW-224D- 0ortiswitch- 0FORTI- 210916/26 0FOE, FSW-248D-POE, FSW- 244D, FSW-248D-FPOE, FSW- 448D, FSW-424D-POE, FSW-448D-FPOE, FSW- 524D, FSW-524D-FPOE, FSW-544D, FSW- 524D, FSW-524D-FPOE, FOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLinkortiswitch- 0	•		10								
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.Bypass2016-09- 0910Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW- 210916/26http://forti guard.com FORTI- 210916/26O-FOR- FORTI- 210916/260108D-POE, FSW-248D-POE, FSW- FPOE, FSW-248D-FPOE, FSW- A24D, FSW-248D-FPOE, FSW- admin- 424D, FSW-424D-POE, FSW-424D-FPOE, FSW- A48D, FSW-448D-POE, S24D, FSW-544BD-POE, FSW-448D-FPOE, FSW- S24D, FSW-548D- FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLinkO-FOR- FORTI- guard.com foRTI- 210916/26											
and are available in a wide rarge of models to fit any environment.Bypass2016-09-10Fortinet FortiSwitch FSW-http://fortiO-FOR-09108D-POE, FSW-124D,guard.comFORTI-210916/26224D-POE, FSW-224D-ortiswitch-0224D-POE, FSW-248D-POE,rest-6FPOE, FSW-248D-POE,rest-FSW-248D-FPOE, FSW-admin-424D, FSW-424D-POE,account-FSW-248D-FPOE, FSW-exposed-448D, FSW-448D-POE,under-FSW-424D-FPOE, FSW-specific-524D, FSW-524D-FPOE,conditionsFSW-548D, FSW-548D, FSW-548D,FPOE, FSW-1024D, FSW-conditionsFSW-548D, FSW-3032D, andFSW-R-112D-POE models,when in FortiLinkunder.under-											
Bypass2016-09- 0910Fortinet FortiSwitch FSW- 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW- 224D-POE, FSW-224D- ortiswitch- rest- admin- account- FSW-248D-FPOE, FSW- 244D, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- account- FSW-424D, FSW-424D-POE, FSW-424D-FPOE, FSW- admin- account- FSW-424D-FPOE, FSW- admin- account- FSW-448D, FSW-448D-POE, FSW-448D-FPOE, FSW- specific- conditionsO-FOR- FORTI- 210916/26 0Bypass2016-09- 10910FORTI- 210916/26 0210916/26 0Bypass224D-POE, FSW-248D-POE, FSW-248D-FPOE, FSW- 424D, FSW-424D-POE, FSW-448D-FPOE, FSW- 524D, FSW-548D-FPOE, FSW-548D, FSW-548D- FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink0						,					
09 108D-POE, FSW-124D, FSW-124D-POE, FSW- 224D-POE, FSW-224D- FPOE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- 424D, FSW-424D-POE, FSW-424D-FPOE, FSW- account- FSW-448D, FSW-448D-POE, Under- S24D, FSW-548D- FSW-548D, FSW- 524D, FSW-548D- FPOE, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink FSW-1024D, FSW- SW-1024D, FSW- SW-1048D, FSW-1024D, FSW- SW-1048D, FSW-1048D, FSW- SW-1048D, FSW- SW-						O-FOR-					
224D-POE, FSW-224D- FPOE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- 424D, FSW-424D-POE, FSW-424D-FPOE, FSW- exposed- 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 ortiswitch- ortiswi		09		108D-POE, FSW-124D,	guard.com	FORTI-					
FPOE, FSW-248D-POE, FSW-248D-FPOE, FSW- admin- 424D, FSW-424D-POE, account- FSW-424D-FPOE, FSW- exposed- under- FSW-448D-FPOE, FSW- specific- 524D, FSW-524D-FPOE, FSW-548D, FSW-548D- FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLinkrest- admin- admin- admin- admin- admin- account- exposed- under- specific- conditions				FSW-124D-POE, FSW-	/advisory/f	210916/26					
FSW-248D-FPOE, FSW- 424D, FSW-424D-POE, FSW-424D-FPOE, FSW- exposed- under- SPW-448D, FSW-448D-POE, FSW-448D-FPOE, FSW- Specific- 524D, FSW-524D-FPOE, FSW-548D, FSW-548D- FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLinkadmin- account- exposed- under- specific- conditions				224D-POE, FSW-224D-	ortiswitch-	0					
424D, FSW-424D-POE, account- FSW-424D-FPOE, FSW- exposed- under- FSW-448D-FPOE, FSW- specific- 524D, FSW-524D-FPOE, conditions FSW-548D, FSW-548D- FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink											
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				, -	admin-						
448D, FSW-448D-POE, under- FSW-448D-FPOE, FSW- 524D, FSW-524D-FPOE, conditions FSW-548D, FSW-548D- FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink											
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				•							
524D, FSW-524D-FPOE, FSW-548D, FSW-548D- FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink											
FSW-548D, FSW-548D- FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink					•						
FPOE, FSW-1024D, FSW- 1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink					conditions						
1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink				-							
FSW-R-112D-POE models, when in FortiLink											
when in FortiLink											
				managed mode and							
upgraded to 3.4.1, might				5							
allow remote attackers to											
	CV										
Scoring         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10	-	0-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10					
Scale Sca											

Denial of Service2016-09- 117.1389864Denial of Service2016-09- 17.18.27.422194 2.10916/26Denial of Service2016-09- 117.18.27.422196Denial of Service2016-09- 117.18.27.422181 2.1.2.5.5.1.2.5.	Google Android Android is ar smartphones		-	<b>4573</b> bogle for use on mobile devi	ces, such as	
Telephony in Android 5.0.xhttps://anbefore 5.0.2, 5.1.x beforedroid.goog5.1.1, 6.x before 2016-09-lesource.c01, and 7.0 before 2016-om/platfor09-01 allows attackers tom/packagcause a denial of servicees/service(loss of locked-screen 911s/TelephonTTY functionality) via ay/crafted application that+/d1d248modifies the TTY mode byd10cf0349broadcasting an intent,aka internal bug29832693.7482a19dDenial of2016-09-2016-09-Reference: CVE-2016-			7 1	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. <b>Reference: CVE-2016-</b>	droid.goog lesource.c om/platfor m/framew orks/av/ +/97837b b6cbac21 ea679843 a0037779 d3834bed	ANDRO- 210916/26
Gain 2016-09- 4.3 The WifiEnterpriseConfig http://sour O-GOO-	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. <b>Reference: CVE-2016- 3898</b>	https://an droid.goog lesource.c om/platfor m/packag es/service s/Telephon y/ +/d1d248 d10cf0349 8efb7041f 1a8c9c46 7482a19d	O-GOO- ANDRO- 210916/26 2

Information	11		class in net/wifi/WifiEnterpriseCon fig.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. <b>Reference: CVE-2016-</b> 3897	ce.android .com/secu rity/bulleti n/2016- 09- 01.html	ANDRO- 210916/26 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,	https://an droid.goog lesource.c	
			and 6.x before 2016-09- 01 allows attackers to obtain sensitive	om/platfor m/packag es/apps/E	
			EmailAccountCacheProvid er information via a	mail/ +/cb2dfe4	
Gain	2016-09-		crafted application, aka internal bug 29767043. <b>Reference: CVE-2016-</b>	3f25cb0c3 2cc73aa4 569c0a51	O-GOO- ANDRO- 210916/26
Information	11	4.3	3896	86a4ef43	4
			Integer overflow in the Region::unflatten function in libs/ui/Region.cpp in	https://an droid.goog lesource.c	
			mediaserver in Android 6.x before 2016-09-01	om/platfor	
			and 7.0 before 2016-09-	m/framew orks/nativ	
			01 allows attackers to obtain sensitive	e/ +/363247	
			information via a crafted application, aka internal	929c3510 4b3e5ee9	0-G00-
Quarter	2010.00		bug 29983260.	e637e9dcf	ANDRO-
Overflow Gain Info	2016-09- 11	4.3	Reference: CVE-2016- 3895	579080ae e	210916/26 5
Gain	2016-09-	4.3	The Qualcomm DMA	http://sour	0-G00-
Information	11		component in Android before 2016-09-05 on	ce.android	ANDRO-
			DEIDIE 2010-09-02 011	.com/secu	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
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

			Nexus 6 devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 29618014 and Qualcomm internal bug CR1042033. <b>Reference: CVE-2016-</b> <b>3894</b>	rity/bulleti n/2016- 09- 01.html	6
Gain Information	2016-09- 11	4.3	The wcdcal_hwdep_ioctl_share d 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. <b>Reference: CVE-2016- 3893</b>	https://sou rce.codea urora.org/ quic/la/ker nel/msm- 3.10/com mit/? id=a7a6d dc91cce7a d5ad55c9 709b24bfc 80f5ac873	O-GOO- ANDRO- 210916/26 7
Gain Information Gain Privileges	2016-09- 11 2016-09- 11	<u>4.3</u> 7.6	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. <b>Reference: CVE-2016- 3892</b> The Java Debug Wire Protocol (JDWP) implementation in adb/sockets.cpp in Android 4.x before 4.4.4,	http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html http://sour ce.android .com/secu rity/bulleti n/2016-	O-GOO- ANDRO- 210916/26 8 O-GOO- ANDRO- 210916/26 9

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. <b>Reference: CVE-2016-</b> <b>3890</b>	09- 01.html	
Bypass Bypass	2016-09- 11 2016-09- 11	7.2 2.1	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. <b>Reference: CVE-2016- 3889</b> internal/telephony/SMSDis patcher.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.	http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html https://an droid.goog lesource.c om/platfor m/framew orks/opt/te lephony/ +/b8d1ae e993dcc5 65e6576b 2f2439a8f 5a507cff6	O-GOO- ANDRO- 210916/27 0 O-GOO- ANDRO- 210916/27 1

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

Bypass116.8 <b>3887</b> 1d5f751d02Bypass116.8 <b>3887</b> 1d5f751d02Systemui/statusbar/phone /QuickStatusBarHeader.ja va in the System UI Tuner in Android 7.0 beforehttps://an droid.goog prevent tuner changes on the lockscreen, which allows physically proximate attackers to gain privileges by modifying a setting, aka internal bug 30107438.alova for a setting, aka a 50311d5o-GOO- o-GOO-Gain Privileges2016-09-9.3debuggerd/debuggerd.cp p 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 7.00om/platfor modifying a setting droid.goog				Reference: CVE-2016-		
Gain Privileges2016-09-01 ADDEhttps://an 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.https://an diof77b C-GOO- ce8a8804 ANDRO- 2016-09-Bypass016.096.83887105751002Bypass106.83887105751002Bypass0116.83887105751002Bypass0116.83887105751002Bypass0116.83887105751002Bypass116.83887105751002Bypass116.83887105751002Bypass117.0 before prevent tuner changes on the lockscreen, which allows physically proximate attackers to modifying a setting, aka internal bug 30107438.0-GOO- a50311d50-GOO- O-GOO- O-GOO-Gain Privileges2016-09-9.3debuggerd/debuggerd.cp p in Debuggerd in Android 5.0.x before 5.0.2, 5.1.x.0-GOO- before 5.1.4 before before 5.0.2, 5.1.x0-GOO- droid.goog ANDRO-Gain Privileges2016-09-9.3debuggerd/debuggerd.cp p in Debuggerd in Android c.0.x before 5.0.2, 5.1.x.0-GOO- droid.goog droid.googGain Privileges2016-09-01, and 7.0m/system/0-GOO-						
J.systemui/statusbar/phone /QuickStatusBarHeader.ja va in the System UI Tuner in Android 7.0 before prevent tuner changes on the lockscreen, which allows physically proximate attackers to gain privileges by https://an droid.goog lesource.c orks/base/ +/6ca6cd5 a50311d5O-GOO- O-GOO- ANDRO- 210916/27Gain Privileges2016-09- 117.2 <b>3886</b> 9eadcd53Gain Privileges2016-09- 119.3debuggerd/debuggerd.cp p 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 7.00-GOO- Mrystem/	Bynass		6.8	sProvider.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. <b>Reference: CVE-2016-</b>	droid.goog lesource.c om/platfor m/framew orks/base/ +/335702 d106797b ce8a8804 4783fa1fc	ANDRO- 210916/27
Gain Privileges2016-09- 17.238869eadcd5Gain Privileges2016-09- 17.238869eadcd5Gain Privileges2016-09- 19.3debuggerd/debuggerd.cp pin Debuggerd in Android 30.2, 5.1.xhttps://an droid.goog https://an om/platfor allows physically biologin proving a setting and allows physically0-GOO- 30107438.Gain Privileges2016-09- 17.238869eadcd5Gain Privileges2016-09- 19.3debuggerd/debuggerd.cp pin Debuggerd in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.00-GOO- Mysystem/	bypass		0.0		1031/3100	۷
Privileges11p 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 7.0droid.goog lesource.cANDRO- 210916/27 d	Privileges	11		/QuickStatusBarHeader.ja va 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. <b>Reference: CVE-2016- 3886</b>	droid.goog lesource.c om/platfor m/framew orks/base/ +/6ca6cd5 a50311d5 8a1b7bf8f bef3f9aa2 9eadcd5	ANDRO- 210916/27 3
mishandles the +/d76035 interaction between 83f90c2bc PTRACE_ATTACH 6074a4ee operations and thread 2886bd28 exits, which allows 082d7c65 attackers to gain b privileges via a crafted application, aka internal			9.3	p 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	droid.goog lesource.c om/platfor m/system/ core/ +/d76035 83f90c2bc 6074a4ee 2886bd28 082d7c65	ANDRO- 210916/27

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/Notifica tionManagerService.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. <b>Reference: CVE-2016- 3884</b>	https://an droid.goog lesource.c om/platfor m/framew orks/base/ +/61e910 3b572596 5568e466 57f4781dd 8f2e5b623	O-GOO- ANDRO- 210916/27 5
NA	2016-09- 11	4.3	internal/telephony/SMSDis patcher.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. <b>Reference: CVE-2016- 3883</b>	https://an droid.goog lesource.c om/platfor m/framew orks/opt/te lephony/ +/b2c89e 6f8962dc7 aff88cb38 aa3ee67d 751edda9	O-GOO- ANDRO- 210916/27 6
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://an droid.goog lesource.c om/platfor m/external /libvpx/ +/4974dc bd0289a2	O-GOO- ANDRO- 210916/27 7
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. <b>Reference: CVE-2016-</b> <b>3881</b>	530df2ee2 a25b5f927 75df80da	
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. <b>Reference: CVE-2016- 3880</b>	https://an droid.goog lesource.c om/platfor m/framew orks/av/ +/68f67ef 6cf1f41e7 7337be3b c4bff91f3a 3c6324	O-GOO- ANDRO- 210916/27 8
Denial of Service Denial of	2016-09- 11 2016-09-	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. <b>Reference: CVE-2016- 3879</b>	https://an droid.goog lesource.c om/platfor m/external /sonivox/ +/cadfb7a 3c96d4fef 06656cf37 143e1b3e 62cae86 https://an	O-GOO- ANDRO- 210916/27 9 O-GOO-
Service	2010-09-	7.1	decoder/ih264d_api.c in mediaserver in Android	https://an droid.goog	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. <b>Reference: CVE-2016-</b> <b>3878</b>	lesource.c om/platfor m/external /libavc/ +/7109ce 3f8f90a28 ca9f0ee6e 14f6ac5e4 14c62cf	210916/28 0
NA	2016-09- 11	10	Unspecified vulnerability in Android before 2016- 09-01 has unknown impact and attack vectors. <b>Reference: CVE-2016-</b> <b>3877</b>	http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html	O-GOO- ANDRO- 210916/28 1
Bypass	2016-09-	7.2	providers/settings/Setting sProvider.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. <b>Reference: CVE-2016- 3876</b>	https://an droid.goog lesource.c om/platfor m/framew orks/base/ +/91fc934 bb2e5ea5 9929bb2f5 74de6db9 b5100745	O-GOO- ANDRO- 210916/28 2
Bypass	2016-09- 11	7.2	server/wm/WindowManag erService.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://an droid.goog lesource.c om/platfor m/framew orks/base/ +/69729fa 8b13cadbf 3173fe1f3 89fe4f3b7 bd0f9c	O-GOO- ANDRO- 210916/28 3
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	2	016-09- 016-09- 11	9.3	<b>3873</b> Buffer overflow in codecs/on2/dec/SoftVPX.c pp 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. <b>Reference: CVE-2016- 3872</b>	http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html	5 O-GOO- ANDRO- 210916/28 6
			9.3	3873		5
Gain Privileges		016-09-		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. <b>Reference: CVE-2016-</b>	http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html	O-GOO- ANDRO- 210916/28
Gain Privileges		016-09-	9.3	vectors, aka internal bug 26251884. <b>Reference: CVE-2016- 3875</b> 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. <b>Reference: CVE-2016- 3874</b>	http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html	O-GOO- ANDRO- 210916/28 4

Overflow; Gain Privileges	2016-09- 11	9.3	Multiple buffer overflows in codecs/mp3dec/SoftMP3.c pp 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. <b>Reference: CVE-2016- 3871</b>	https://an droid.goog lesource.c om/platfor m/framew orks/av/ +/c2639af ac631f5c1 ffddf70ee8 a6fe943d0 bedf9	O-GOO- ANDRO- 210916/28 7
Gain Privileges	2016-09- 11	9.3	omx/SimpleSoftOMXComp onent.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. <b>Reference: CVE-2016- 3870</b>	https://an droid.goog lesource.c om/platfor m/framew orks/av/ +/1e9801 78377091 7728b7ed bdeff3d0e c09c621ac	O-GOO- ANDRO- 210916/28 8
Gain Privileges Gain	2016-09- 11 2016-09-	9.3 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. <b>Reference: CVE-2016- 3869</b> The Qualcomm power	http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html http://sour	O-GOO- ANDRO- 210916/28 9 O-GOO-

/ <b>0-1 1-2 2-</b> coring <b>0-1 1-2 2-</b> cale	3-4 4-5	5-6 6-7	7-8 8-9	9-10
---	---------	---------	---------	------

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 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. <b>Reference: CVE-2016- 3865</b>	http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html	O-GOO- ANDRO- 210916/29 3
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. <b>Reference: CVE-2016- 3866</b>	http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html	O-GOO- ANDRO- 210916/29 2
Privileges Gain Privileges	11 2016-09- 11	9.3	bug CR1032875. <b>Reference: CVE-2016- 3868</b> 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. <b>Reference: CVE-2016- 3867</b>	n/2016- 09- 01.html http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html	ANDRO- 210916/29 0 0 O-GOO- ANDRO- 210916/29 1
			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	ce.android .com/secu rity/bulleti	

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. <b>Reference: CVE-2016- 3864</b>	http://sour ce.android .com/secu rity/bulleti n/2016- 09- 01.html	O-GOO- ANDRO- 210916/29 4
Execute Code; Overflow	2016-09-	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. <b>Reference: CVE-2016- 3863</b>	https://an droid.goog lesource.c om/platfor m/framew orks/av/ +/119a01 2b2a9a18 6655da4b ef3ed4ed8 dd9b94c2 6	O-GOO- ANDRO- 210916/29 5
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://an droid.goog lesource.c om/platfor m/framew orks/base/ +/e739d9 ca5469ed 30129d0fa 228e3d0f2 878671ac	O-GOO- ANDRO- 210916/29 6

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

				crafted internal <b>Refere</b> <b>3862</b>		270469					
Denial of Service; Execute Code; Overflow	20	016-09- 11	9.3	5.0.2, 5 6.x befo and 7.0 01 mish convers Unicode encodin encodin	1.4.4, 5.0 1.x before 2 before 2 andles ions bet charact g widths emote a ute arbit e a denia (heap-b verflow) file, aka 250543.	0.x befor ore 5.1. -09-01, 2016-09 ween ter differen s, which ttacker trary co al of ased via a interna	1, )- nt s de Il	dro les on m/ co +/0 8a ce 45	ps://an bid.goog ource.c n/platfor system/ re/ ecf5fd5 8f50362 9e8d42 a33d56 f142b	2 O-0 AN	500- DRO- D916/29
Gain Privileges Overflow; Gain Privileges		016-09- 11 016-09- 11	9.3 9.3	The Qua driver in 2016-09 5X, 6, a allows a privilege applicat internal and Qua bug CR <b>Referen</b> <b>3859</b> Buffer o drivers/s em_rest Qualcor driver in 2016-09 and 6P o attacket	n Android -05 on l nd 6P de ittackers es via a ion, aka bug 288 alcomm L034641 nce: CV verflow soc/qcor art.c in nm subs n Android -05 on l devices	d before Nexus 5 evices to gair crafted Androi 315326 interna ( <b>E-2016</b> in m/subsy the system d before Nexus 5 allows n	e 5, d l <b>5-</b> yst e 5X	htt ce .cc n/2 09 01 htt rce qu ne 3.1 mi id=	p://sour androic m/secu y/bulleti 2016- - .html ps://sou codea pra.org/ ic/la/ker l/msm- L0/com	O-0 AN 210 8 0-0 AN 210	500- DRO- )916/29 500- DRO- )916/29
CV	0-1	1-2	2-3	3-4	4-5	5-6	6-7	,	7-8	8-9	9-10

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

Gain2016-09- InformationThe TLS implementation in HPE Integrated Lights- Out 3 (aka iLO 3) firmware properly use a MAC protection mechanism in conjunction with CBC 2.hpe.com padding, which allows (portal/site information via a padding- oracle attack, aka a Vaudenay attack.https://h2 Service, Integrated Lights-out 3Gain2016-09- 084.343790-HP- INTEG- 210916/3CInformation084.343790Information087.5Multiple unspecified vulnerabilities in HPE Integrated Lights-out 3https://h2 INTEG- 210916/3C0-HP- INTEG- 210916/3CDenial of Gain2016-09- 2016-09-7.5Multiple unspecified vulnerabilities in HPE Integrated Lights-Out 3https://h2 INTEG- 210916/3C0-HP- INTEG- 210916/3CInformation7.5Multiple unspecified vulnerabilities in HPE Integrated Lights-Out 3https://h2 INTEG- 210916/3C0-HP- INTEG- 210916/3CInformation6ain (aka iLO 3) firmware before 1.88, Integrated Lights-Out 4https://h2 (bc/publ ic/kb/docD0-HP- INTEG- 210916/3CInformation7.5Multiple unspecified vulnerabilities in HPE before 2.32 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via unknown vectors.n-a- c05236950	HP Integrated server.	Ligh	ts-out	3 Firr	internal and Qua bug CR: <b>Refere</b> 3858 mware:	tring, al bug 28 alcomm 1022641 <b>nce: CV</b>	ka Andr 675151 interna <b>(E-201</b> 0 itates r	oid II 6- emot	0f 4b e3		6	t of	
Integrated Lights-out 4 Mrca Firmware <i>iLO facilitates remote management of server.</i> Denial of Service; Gain Information2016-09- 87.5Multiple 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 unknownhttps://h2 O-HP- INTEG- 2.hpe.com 2.hpe.com /portal/site 1	Information		08		in HPE I Out 3 (a before 1 properly protecti conjunc padding remote obtain s informa oracle a Vaudena <b>Refere</b> 4379	ntegrate aka iLO3 L.88 doe / use a l on mech tion with attacket sensitive tion via attack, a ay attac <b>nce: CV</b>	ed Light ) firmw s not MAC nanism n CBC allows rs to a padd ka a k. <b>(E-201</b> )	ts- are in ing- <b>6-</b>	05 2.1 /pc /hj ic/ isp do r_r c0 0	66.www npe.com ortal/sit osc/pub kb/doc[ olay? cld=em na- 524976	v e l D D I S 2 0	NTE 109	G- 916/30
Denial of Service; Gain Information2016-09- 087.5Multiple 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 unknownhttps://h2 0.566.www (D.HP- D.S66.www 2.hpe.com /portal/site 1O-HP- INTEG- 210916/30 1Denial of Service via unknown0	Integrated	Ligh	ts-out	4 Mrc	a Firmv	vare	ted Lig	ghts-	ou	t 4 Firi	mwa	ire;	
	Denial of Service; Gain		)16-09-		Multiple vulnera Integrat (aka iLC before 1 Lights-C firmwar Integrat (aka iLC firmwar allow re obtain s informa or cause	e unspec bilities in ed Light 3) firm 1.88, Int 2014 (al e before ed Light e before mote at ensitive tion, mo e a deni- via unkr	h HPE s-Out 3 ware egrated a iLO 4 2.44, a s-Out 4 2 2 2 2 2 4 2 2 3 2 4 3 2 3 2 3 2 3 2	d l) and 4 s to	05 2.1 /pc /hj ic/ isp do r_r c0	66.www npe.com ortal/sit osc/pub kb/doc[ olay? cld=em na-	v IN n 2 e 1 J D	NTE 109	G-

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

			Reference: CVE-2016- 4375		
Huawei				<u> </u>	<u> </u>
Ch121 V3 S	erver Firm	ware;	Ch140 V3 Server Firmwa	re;Ch220 V3	<b>3 Server</b>
			Firmware;Ch226 V3 Serv		
			8 V3 Server Firmware;X6		
Firmware;X	h620 V3 Se	rver	Firmware		
The HUAWEI	RH series	is a r	new-generation 1U dual-soc	ket rack ser	ver; Huawe
Fusion Serve	r XH Server	serie	s is a full-height dual-socket	server node.	
			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	http://www	
			encrypted data and	.huawei.co	
			consequently obtain	m/en/psirt	
			sensitive information by	/security-	
			leveraging selection of an	advisories/	
			insecure SSH encryption	huawei-sa-	O-HUA-
Calia	2016 00		algorithm.	20160817-	CH121-
Gain	2016-09-	4 2	Reference: CVE-2016-	02-server-	210916/30
Information Honor 4c Fi	07	4.3	6838	en	2

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 Denial of Service ;	2016-09- 07 2016-09- 07	6.9 9.3	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. <b>Reference: CVE-2016- 6183</b> The Camera driver in Huawei Honor 4C	http://www .huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160716- 01- smartphon e-en http://www .huawei.co	O-HUA- HONOR- 210916/30 4 O-HUA- HONOR-
Service ; Gain Privileges	07		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. <b>Reference: CVE-2016-</b> <b>6183</b>	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160716- 01- smartphon e-en	HONOR- 210916/30 4
			Huawei Honor 4C smartphones with software CHM-UL00C00		
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. <b>Reference: CVE-2016-</b> <b>6184</b> The Camera driver in	http://www .huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160716- 01- smartphon e-en	O-HUA- HONOR- 210916/30 3

oring 0-1 1-2 2- ale	3-4 4-5 5-6	<b>6</b> 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. <b>Reference: CVE-2016-</b> <b>6182</b>	m/en/psirt /security- advisories/ huawei-sa- 20160716- 01- smartphon e-en	210916/30 5
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- TL00C01 before 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. <b>Reference: CVE-2016-</b> <b>6181</b>	http://www .huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160716- 01- smartphon e-en	O-HUA- HONOR- 210916/30 6
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.co m/en/psirt /security-	O-HUA- HONOR- 210916/30 7

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. <b>Reference: CVE-2016-</b> <b>6180</b> The WiFi driver in Huawei Honor 6 smartphones with software H60-L01	advisories/ huawei-sa- 20160716- 01- smartphon e-en	
Denial of Service ; Gain Privileges	2016-09- 07		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. <b>Reference: CVE-2016- 6179</b>	http://www .huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160713- 01- smartphon e-en	HONOR- 210916/30 8
Server Firm Xh622 V3 S	nware;Rh58 Server Firm	85 V. ware;	re;Rh2288 V3 Server F 3 Server Firmware;Xh62 Xh628 V3 Server Firmwa new-generation 1U dual-soo	0 V3 Servei ire	Firmware;
			is a full-height dual-socket		
Denial of Service	2016-09- 07		The Intelligent Baseboard Management Controller (iBMC) in Huawei RH1288 V3 servers with software	http://www .huawei.co m/en/psirt /security-	O-HUA- RH128- 210916/30 9
CV					

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		
			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	http://www	
			V100R003C00SPC515	.huawei.co	
			allow remote attackers to	m/en/psirt	
			obtain passwords via a	/security-	
			brute-force attack, related	advisories/	
			to "lack of authentication	huawei-sa-	O-HUA-
			protection mechanisms."	20160817-	RH128-
	2016-09-		Reference: CVE-2016-	01-server-	210916/31
NA	2010-09-	5	6825	en	1
			nware;S9700 Firmware/S		_ <b>_</b>
			outing Switches for campus r		o 50300 is a
			h six service slots. It is highl		
			high availability.	y readination	to meet
	regan criterie	5 101 1	ngn avanabilityi		
Gain				http://www	O-HUA-
Gain Information	2016-09-		Huawei S7700, S9300,	http://www	
Gain Information			Huawei S7700, S9300, S9700, and S12700	.huawei.co	S7700-
	2016-09-		Huawei S7700, S9300, S9700, and S12700 devices with software	.huawei.co m/en/psirt	S7700- 210916/31
	2016-09-		Huawei S7700, S9300, S9700, and S12700 devices with software before	.huawei.co m/en/psirt /security-	S7700-
	2016-09-		Huawei S7700, S9300, S9700, and S12700 devices with software before V200R008C00SPC500 use	.huawei.co m/en/psirt /security- advisories/	S7700- 210916/31
	2016-09-		Huawei S7700, S9300, S9700, and S12700 devices with software before V200R008C00SPC500 use random numbers with	.huawei.co m/en/psirt /security- advisories/ huawei-sa-	S7700- 210916/31
	2016-09-		Huawei S7700, S9300, S9700, and S12700 devices with software before V200R008C00SPC500 use random numbers with insufficient entropy to	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160810-	S7700- 210916/31
	2016-09-		Huawei S7700, S9300, S9700, and S12700 devices with software before V200R008C00SPC500 use random numbers with insufficient entropy to generate self-signed	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160810- 01-	S7700- 210916/31
	2016-09-		Huawei S7700, S9300, S9700, and S12700 devices with software before V200R008C00SPC500 use random numbers with insufficient entropy to generate self-signed certificates, which makes	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160810- 01- certificate-	S7700- 210916/31
	2016-09-		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	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160810- 01-	S7700- 210916/31
	2016-09-		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	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160810- 01- certificate-	S7700- 210916/31
	2016-09-		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	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160810- 01- certificate-	S7700- 210916/31
	2016-09-		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	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160810- 01- certificate-	S7700- 210916/31
	2016-09-		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	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160810- 01- certificate-	S7700- 210916/31
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.	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160810- 01- certificate- en	\$7700- 210916/31 2
Information	2016-09-		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.	.huawei.co m/en/psirt /security- advisories/ huawei-sa- 20160810- 01- certificate- en	S7700- 210916/31

			Reference: CVE-2016-		
			6670		
IBM Mg Applian	co Eirmwor	•			
Mq Applian			e application connectivity pe	rformance of	FIBM MO
			ng 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. <b>Reference: CVE-2016-</b> <b>5879</b>	http://ww w- 01.ibm.co m/support /docview. wss? uid=swg2 1987697	O-IBM-MQ AP- 210916/31 3
Juniper					
	uters. It is an d security de	oper vices		Juniper's rou	ting,
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.j uniper.net/ InfoCenter /index? page=con tent&id=J SA10755	O-JUN- JUNOS- 210916/31 4
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	2016-09-		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 14.1R7, 14.1X53 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. <b>Reference: CVE-2016-</b>	http://kb.j uniper.net/ InfoCenter /index? page=con tent&id=J	O-JUN- JUNOS- 210916/31
Information	09	10	1279	SA10754	5
Denial of	2016.00		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.	http://kb.j uniper.net/ InfoCenter /index? page=con	O-JUN- JUNOS- 210916/31
Denial of Service	2016-09- 09	7.1	Reference: CVE-2016- 1277	tent&id=J SA10752	210916/31 6

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 Juno 13.3R9, 14.1 14.1R6-S1, a before 14.11 configured v routing-insta remote atta obtain sensi information flood of Ethe with IPv6 M directly into interface. <b>Reference:</b> <b>1275</b>	1R6 before and 14.1 R7, when with VPLS ances, allow ckers to tive mbuf by injecting ernet frame AC address a connector <b>CVE-201</b>	ws g a es es ed <b>6-</b>	http://kb.j uniper.net/ InfoCenter /index? page=con tent&id=J SA10750	O-JU JUN(	
Denial of Service	2016-09- 09		Juniper Juno 12.1X46-D4 D50, 12.1X4 12.1X47-D3 before 12.33 before 13.31 before 14.11 before 14.11 before 15.11 before 16.11 before 16.11 before 17.11 before 17.11 before 16.11 before 17.11 before 18.11 before 18.	5, 12.1X46 7 before 5, 12.3X48 X48-D30, 1 R9-S1, 14.1 R7, 14.2 R6, 15.1 =2-S5, 15.1 R2-S3, 15.1 R3, and fore 15.1X4 emote cause a rvice (kerne crafted UD ined to the address of evice.	- 3.3 F4 .R I9- el P a <b>6-</b>	http://kb.j uniper.net/ InfoCenter /index? page=con tent&id=J SA10758	O-JU JUN(	
Linux	05	7.0	1205			5/(10/50		
Linux Kerne	el							
The Linux ke operating sy	ernel is a Unix stem is base conal comput 2016-08- 30	d on it ers and 10	and deploy	ed on both sually in the eger overflo	tradit e form ows	tional comp	uter s	i <mark>tions</mark> N-
CV Scoring Scale	0-1 1-2	2-3	3-4 4	-5 5-6	6-7	7-8	8-9	9-10

Overflow			in Qualo Center ( contribu devices product to cause service unspeci via a lar related mdss_co mdss_ft mdss_ro	ompat_u	novatio ndroid r MSM er attacke al of bly hav er impa value, utils.c,	on ers re ict	eg ov mo dr	a.org/inf jer- erflow- dss- iver-cve 016-534	- 210	916/31
Denial of			Heap-ba overflov wcnss_v functior drivers/ /wcnss_v wcnss_v for the I as used Innovat Android MSM de product to cause service unspeci by writin /dev/wc	wlan_wr n in net/wire wlan.c i wlan dev Linux ke in Qual ion Cent contrib vices ar s, allows e a deni or possi fied oth	te less/wo n the vice driv rnel 3.> comm comm er (Qul utions f d othe s attack al of bly hav er impa n with a	ver (, C) for r kers r kers nct	ht: w.i ffe ov vu ty·	tps://ww codeaur a.org/bu er- 'erflow- ilnerabil	i O-Ll	
Service; Overflow	2016-08-		Refere	nce: CV	'E-201	6-	wr	ite-cve-	210	916/32
Microsoft	30	1.2	5342				20	16-5342	2   0	
Windows 1										
Windows 10 Microsoft as	is a persona								release	ed by
Denial of	2016-09-			ft Windo				tp://tech	n O-M	IC-
Service	14			d 1511				et.micros		DO-
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 via	
unspecified vectors, a	ka oft.com/en
"Windows Denial of	- ,
Service Vulnerability." Reference: CVE-201	us/securit   <b>6-</b> y/bulletin/ 210916/32
Overflow 3369	6- y/bulletin/ 210916/32 ms16-110 1
The Graphics Device	
Interface (GDI) in	
Microsoft Windows 10	
1607 allows remote attackers to execute	http://toch
arbitrary code via a	http://tech net.micros
crafted document, aka	
"GDI Remote Code	- O-MIC-
Execute Execution Vulnerability	
Code;         2016-09-         Reference: CVE-201           Overflow         14         9.3         3356	6- y/bulletin/ 210916/32 ms16-106 2
Microsoft Windows 10	111510-100 2
Gold, 1511, and 1607	
does not properly enfo	orce
permissions, which all	ows
local users to obtain Administrator access v	via a http://tech
crafted DLL, aka	net.micros
"Windows Permissions	
Enforcement Elevation	
Privilege Vulnerability.	
2016-09-         Reference: CVE-201           NA         14         7.2         3346	6- y/bulletin/ 210916/32 ms16-110 3
The Secure Kernel Mod	
feature in Microsoft	
Windows 10 Gold and	
1511 allows local user obtain sensitive	S TO
information via a craft	ed http://tech
application, aka "Wind	
Secure Kernel Mode	oft.com/en
Information Disclosure	
Gain 2016-09- <b>Reference: CVE-201</b>	us/securit WINDO- 6- y/bulletin/ 210916/32
Information 14 2.1 3344	ms16-113 4

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.

Jerver series		vviiriu	ows server line of operating	systems.	
			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	http://tech	
			crafted application, aka	net.micros	
			"Windows Kernel	oft.com/en	
			Elevation of Privilege	-	O-MIC-
			Vulnerability."	us/securit	WINDO-
Gain	2016-09-		Reference: CVE-2016-	y/bulletin/	210916/32
Information	14	4.3	3373	ms16-111	5
			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	http://tech	
			crafted application, aka	net.micros	
			"Windows Kernel	oft.com/en	
			Elevation of Privilege	-	O-MIC-
			Vulnerability."	us/securit	WINDO-
Gain	2016-09-		Reference: CVE-2016-	y/bulletin/	210916/32
Information	14	4.3	3371	ms16-111	6
mornation	<u> </u>	1.5	<i></i>		~

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." <b>Reference: CVE-2016- 3368</b>	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-110	O-MIC- WINDO- 210916/32 7
Gain Privileges Bypass	2016-09- 14 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." <b>Reference: CVE-2016- 3355</b> The Graphics Device Interface (GDI) in	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-106 http://tech net.micros	O-MIC- WINDO- 210916/32 8 O-MIC- WINDO-
	14		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	net.micros oft.com/en - us/securit y/bulletin/ ms16-106	WINDO- 210916/32 9

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	9.3	3348 The SMBv1 server in Microsoft Windows Vista SP2, Windows Server	ms16-106	0
Gain Privileges	2016-09- 14	9.3	Privilege Vulnerability." <b>Reference: CVE-2016-</b> <b>3348</b> The SMBv1 server in	us/securit y/bulletin/ ms16-106	WINDO- 210916/33 0
			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	http://tech net.micros oft.com/en	O-MIC-
			The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1,		
			a crafted application, aka "GDI Information Disclosure Vulnerability." <b>Reference: CVE-2016-</b> <b>3354</b>		
			Gold, 1511, and 1607 allows local users to bypass the ASLR protection mechanism via		

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 NA	2016-09- 14 2016-09- 14	<u>4.6</u> 4.3	than CVE-2016-3306. <b>Reference: CVE-2016-</b> <b>3305</b> Microsoft Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511,	us/securit y/bulletin/ ms16-111 http://tech net.micros oft.com/en	WINDO- 210916/33 3 O-MIC- WINDO- 210916/33
			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	http://tech net.micros oft.com/en	O-MIC-
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. <b>Reference: CVE-2016- 3306</b>	net.micros oft.com/en - us/securit y/bulletin/ ms16-111	WINDO- 210916/33 2

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

Windows 1	0;Windows	8.1;V	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." <b>Reference: CVE-2016-</b> <b>3352</b> Vindows Rt 8.1; Windows	- us/securit y/bulletin/ ms16-110 Server 2012	4
Windows is a	metafamily	of gra	aphical operating systems de	eveloped, ma	arketed, and
			f several families of operatin lows server line of operating		IIIUUWS
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." <b>Reference: CVE-2016- 3349</b>	http://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-106	O-MIC- WINDO- 210916/33 5
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://tech net.micros oft.com/en - us/securit y/bulletin/ ms16-112	O-MIC- WINDO- 210916/33 6

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

			Privilege <b>Refere</b>							
			3302							
	erver 2008;									
	a metafamily									
-	osoft. It cons				-				Nindo	WS
Server series	<mark>s is Microsoft</mark>	vvina	<u>ows serv</u> The ker				sys	stems.		
			Window							
			Window							
			does no			-				
			permiss							
				ers to sp						
			•	es, spoc						
			process or cause			n,	<b>h</b> +	tp://tech		
			service					et.micros		
			applicat			ows		t.com/er		
			Kernel E			00	-			MIC-
			Privilege	e Vulner	ability."	I	us	s/securit	WI	NDO-
Denial of	2016-09-		Refere	nce: CV	E-201	6-	-	bulletin/		0916/33
Service	14	3.6	3372				m	s16-111	7	
Моха					-		•			
Oncell G30	01 Firmwar	e; On				re:N	A			
			Moxa O devices							
			G3111,							
			and G32							
			1.7 use	cleartex	t					
			passwo							
			makes i					tps://ics	-	
			users to					ert.us-		
			informa configui			d		ert.gov/a /isories/l		MOX- CEL-
Gain	2016-08-		Refere			6-		5A-16-		0916/33
Information	23	2.1	5812	••				36-01	8	,
NA	2016-08-	10	Moxa O					tps://ics		MOX-
	23		devices					ert.us-		CEL-
			G3111,	•				ert.gov/a		0916/33
			and G32 1.7 do r			ore		visories/I 5A-16-	9	
			restrict		-			36-01		
			attempt			s it				
			easier f							
CV										
Scoring	0-1 1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10
Scale										

			1	
		attackers to obtain access via a brute-force attack.		
		Reference: CVE-2016-		
		5799		
Nuuo				
Nvrmini 2;N		weight, portable NVR solution	with NAS fun	ctionalitv:
	-	b hassle free, lightweight NVR		<b>,</b>
		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		
			http://www	O-NUU-
		access via unspecified vectors.	.kb.cert.or	NVRMI-
	2016-08-	Reference: CVE-2016-	g/vuls/id/8	210916/34
NA	31 1		56152	0
Vmware				-
Photon OS				
	a minimal Linux	<i>container host, optimized to</i>	run on VMwa	re
platforms.				
		VMware Photos OS OVA		
		1.0 before 2016-08-14		
		has a default SSH public		
		key in an authorized_keys		
		file, which allows remote	http://www	
		attackers to obtain SSH	.vmware.c	
		access by leveraging knowledge of the private	om/securit	O-VMW-
		key.	y/advisori es/VMSA-	PHOTO-
			-	111010-
NA	2016-08-	Reference: CVF-2016-	2016-	210916/34
	2016-08- 30 9.	Reference: CVE-2016- 3 5333	2016- 0012.html	210916/34 1
	30 9.	3 5333	0012.html	
	30 9. Applicat		0012.html	
Canonical/	30 9. Applicati Qemu	3 5333	0012.html	
Canonical/ Ubuntu Lin	30 9. Applicati Qemu ux/Qemu	5333 ion; Operating System	0012.html (A/OS)	1
Canonical/ Ubuntu Linu	30 9. Applicati Qemu ux/Qemu x is an Operating	3 5333	0012.html (A/OS) valization who	1 en
Canonical/ Ubuntu Linu	30 9. Applicati Qemu ux/Qemu x is an Operating	<b>5333</b> <b>ion; Operating System</b> <i>g System/ QEMU supports virtu</i> pervisor or using the KVM kern	0012.html (A/OS) valization who	1 en
Canonical/ Ubuntu Linux executing ur	30 9. Application Qemu ux/Qemu x is an Operating order the Xen hyp	<b>5333</b> <b>ion; Operating System</b> <i>g System/ QEMU supports virtu</i> pervisor or using the KVM kern	0012.html (A/OS) valization who el module in	1 en Linux.
Canonical/ Ubuntu Linu Ubuntu Linu executing ur Denial of	30 9. Application Qemu ux/Qemu x is an Operating order the Xen hyp 2016-09- 1.	5 5333 5 5333 5 5333 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	0012.html (A/OS) valization who el module in https://bu	1 en Linux. A-OS-CAN-
Canonical/ Ubuntu Linu Ubuntu Linu executing ur Denial of	30 9. Application Qemu ux/Qemu x is an Operating order the Xen hyp 2016-09- 1.	<ul> <li>5333</li> <li>5333</li> <li>ion; Operating System</li> <li>System/ QEMU supports virtupervisor or using the KVM kern</li> <li>The megasas_lookup_frame</li> </ul>	0012.html (A/OS) valization who el module in https://bu gzilla.redh	1 en Linux. A-OS-CAN- UBUNT-
Canonical/ Ubuntu Linux executing ur Denial of Service	30 9. Application Qemu ux/Qemu x is an Operating oder the Xen hyp 2016-09- 02	<ul> <li>5333</li> <li>5333</li> <li>5 Operating System</li> <li>5 System/ QEMU supports virtupervisor or using the KVM kern</li> <li>5 The megasas_lookup_frame function in QEMU, when built with MegaRAID SAS</li> </ul>	0012.html (A/OS) valization who el module in https://bu gzilla.redh at.com/sh ow_bug.cg	1 en Linux. A-OS-CAN- UBUNT- 210916/34 2
Canonical/ Ubuntu Linux executing ur Denial of Service	30 9. Application Qemu ux/Qemu x is an Operating oder the Xen hyp 2016-09- 02	5 5333 5 5333 5 5333 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	0012.html (A/OS) valization who el module in https://bu gzilla.redh at.com/sh ow_bug.cg	1 en <u>Linux.</u> A-OS-CAN- UBUNT- 210916/34

			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. <b>Reference: CVE-2016-</b>	i? id=13364	
			5107	61	
Denial of Service	2016-09- 02	1.5	The megasas_dcmd_set_prope rties 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. <b>Reference: CVE-2016-</b> <b>5106</b>	https://bu gzilla.redh at.com/sh ow_bug.cg i? id=13395 78	A-OS-CAN- UBUNT- 210916/34 3
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. <b>Reference: CVE-2016-</b> <b>5105</b>	https://bu gzilla.redh at.com/sh ow_bug.cg i? id=13395 83	A-OS-CAN- UBUNT- 210916/34 4

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

Accounting S	olution; The o	penSUS e officia 5	SE project is a worldwide effo al image viewer for the Gnom Eye of GNOME (aka eog) 3.16.5, 3.17.x, 3.18.x	ort that promo	tes the use of ironment. A-OS-CAN-
The Linux I operating sy such as pers Fedora (form developed by	kernel is a stem is base sonal comput nerly Fedora the commun	Unix-lii d on it cers an Core) ity-supp	<b>Opensuse/Eye Of Gnome</b> ke computer operating s and deployed on both trace of servers, usually in the for is an operating system be ported Fedora Project and sp opletely integrated Legal C	ystem kerne ditional comp orm of Linux o ased on the oonsored by Re	uter systems distributions/ Linux kernel, ed Hat. / LEAP
			ovell/Gnome		
Denial of Service Denial of Service; Execute Code <b>Canonical;</b>	2016-09- 02 2016-09- 07 <b>Fedoraproj</b> 0	1.5	Reference: CVE-2016- 4952 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	id=13343 84 http://git.q emu.org/? p=qemu.g it;a=com mit;h=926 cde5f3e4d 2504ed16 1ed0cb77 1ac7cad6f d11	210916/34 5 A-OS-CAN- UBUNT- 210916/34 6
Donial of	2016.00		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_RING S or (2) PVSCSI_CMD_SETUP_MSG _RING SCSI command.	https://bu gzilla.redh at.com/sh ow_bug.cg i?	A-OS-CAN- UBUNT- 210016/24

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- 07	5	idn in GNU libidn before 1.33 might allow remote	http://git.s avannah.g nu.org/cgit /libidn.git/ commit/?	A-OS-CAN- UBUNT- 210916/35 0
Gain Information	2016-09- 07		triggers an out-of-bounds read, a different vulnerability than CVE- 2015-8948. <b>Reference: CVE-2016-</b> 6262	9c7b5bf0c e665b9d6 8f5ddf095 af5c9ba60	A-OS-CAN- UBUNT- 210916/34 9
			idn in libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which	http://git.s avannah.g nu.org/cgit /libidn.git/ commit/? id=5e3cb	
Denial of Service	2016-09- 07		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. <b>Reference: CVE-2016-</b> 6261	http://git.s avannah.g nu.org/cgit /libidn.git/ commit/? id=f20ce1 128fb7f4d 33297eee 307dddaf0 f92ac72d	A-OS-CAN- UBUNT- 210916/34 8
Ubuntu Lin Ubuntu is co a completely openSUSE pro	integrated Leg	<b>pensu</b> e to do gal Cas dwide e	<b>se/Libidn</b> wnload, use and share/ LEA e Management & Legal Accou effort that promotes the use of internationalized domain name	nting Solution f Linux/ GNU's	; The
Cononicali			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. <b>Reference: CVE-2016-</b> 6855	/browse/e og/plain/N EWS? h=3.20.4	210916/34 7

			attackers to obtain		
			sensitive memory		
			information by reading a	id=570e6	
			zero byte as input, which	8886c41c	
			triggers an out-of-bounds	2e765e62	
			read.	18cb317d	
			Reference: CVE-2015-	9a9a447a	
			8948	041	
Debian/Dru					
Debian Lin					
			and a distribution of Free S		oal is a
			b content management and		
experiences	. Drupal prov	ides d	leep capabilities and endles	s flexibility oi	n the web.
			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	https://ww	
			a rebuild of the user	w.drupal.o	A-OS-DEB-
			profile form.	rg/SA-	DEBIA-
Gain	2016-09-		Reference: CVE-2016-	CORE-	210916/35
Privileges	09	6.5	•	-	
Privileges Debian/Ruk	09 Dyonrails		Reference: CVE-2016- 6211	CORE-	210916/35
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On	Rails	Reference: CVE-2016- 6211	CORE- 2016-002	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211	CORE- 2016-002	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On	Rails	Reference: CVE-2016- 6211 System/ Ruby on Rails is ope	CORE- 2016-002	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 System/ Ruby on Rails is ope Cross-site scripting (XSS)	CORE- 2016-002	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 System/ Ruby on Rails is ope Cross-site scripting (XSS) vulnerability in Action	CORE- 2016-002	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 <i>System/ Ruby on Rails is ope</i> Cross-site scripting (XSS) vulnerability in Action View in Ruby on Rails 3.x	CORE- 2016-002	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 System/ Ruby on Rails is ope Cross-site scripting (XSS) vulnerability in Action View in Ruby on Rails 3.x before 3.2.22.3, 4.x	CORE- 2016-002	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 <i>System/ Ruby on Rails is ope</i> 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	CORE- 2016-002 <i>n source soft</i> http://webl	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 <i>System/ Ruby on Rails is ope</i> 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	CORE- 2016-002 <i>n source soft</i> http://webl og.rubyon	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 <i>System/ Ruby on Rails is ope</i> 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	CORE- 2016-002 n source soft http://webl og.rubyon rails.org/2	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 <i>System/ Ruby on Rails is ope</i> 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	CORE- 2016-002 n source soft http://webl og.rubyon rails.org/2 016/8/11/	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 <i>System/ Ruby on Rails is ope</i> 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	CORE- 2016-002 n source soft http://webl og.rubyon rails.org/2	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 <i>System/ Ruby on Rails is ope</i> 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	CORE- 2016-002 n source soft http://webl og.rubyon rails.org/2 016/8/11/	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 System/ Ruby on Rails is ope 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	CORE- 2016-002 n source soft http://webl og.rubyon rails.org/2 016/8/11/ Rails-5-0-	210916/35 1
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 System/ Ruby on Rails is ope 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	CORE- 2016-002 n source soft og.rubyon rails.org/2 016/8/11/ Rails-5-0- 0-1-4-2-7-	210916/35 1 ware to
Privileges Debian/Rut Debian Linu	09 Dyonrails ux/Ruby On x is an Opera	Rails	Reference: CVE-2016- 6211 System/ Ruby on Rails is ope 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 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	CORE- 2016-002 n source soft og.rubyon rails.org/2 016/8/11/ Rails-5-0- 0-1-4-2-7- 2-and-3-2-	210916/35 1 ware to A-OS-DEB- DEBIA-
Privileges Debian/Ruk Debian Linux building web	09 <b>Dyonrails</b> <b>ux/Ruby On</b> <i>x is an Opera</i> <i>application.</i>	Rails	Reference: CVE-2016- 6211 System/ Ruby on Rails is ope Cross-site scripting (XSS) vulnerability in Action View in Ruby on Rails 3.x before 3.2.22.3, 4.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.	CORE- 2016-002 n source soft og.rubyon rails.org/2 016/8/11/ Rails-5-0- 0-1-4-2-7- 2-and-3-2- 22-3-have-	210916/35 1 ware to A-OS-DEB- DEBIA-
Privileges Debian/Ruk Debian Linux building web	09 <b>byonrails</b> <b>ux/Ruby On</b> <i>is an Opera</i> <i>application</i> . 2016-09-	Rails ting S	Reference: CVE-2016- 6211 System/ Ruby on Rails is ope 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-	CORE- 2016-002 n source soft og.rubyon rails.org/2 016/8/11/ Rails-5-0- 0-1-4-2-7- 2-and-3-2- 22-3-have- been-	210916/35 1 ware to A-OS-DEB- DEBIA- 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	
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	--

	reeine									
Fedora/F		Eadara	Corol	ic an an	orating	nuctom	bacad	on tha li	nuv ko	rnol
Fedora (fo										
develope										
Identity a	<u>na Autn</u>	enticati	on soi				- î	a environ	ments.	
				The cer	—					
				in Freell						
				for the '						
					ion, whi		NS			
				remote						
				users to			-			
				certifica				ttps://feo		
				the "ret		rtificate		rahosted		S-FED-
				permiss				rg/freeip	FED	
	20	016-09-		Refere	nce: CV	E-201		/ticket/62		916/35
NA		07	4	5404			32	2	3	
Novell/R	oundcu	ıbe								
Leap/We	bmail									
LEAP Lega		re provid	les a co	ompletely	/ integra	ed Leaa	al Case I	Managem	ent & L	egal
Accounting										
desktop-l										
standard					<i>,</i>	,				
				Cross-si	te reque	est fora	erv			
				(CSRF)						
				Roundci						
					L.1.5 allo	-	h	tps://git		
				remote				ub.com/r		
				the auth				undcube		
				users fo				undcube		
				downloa				ail/com	-	
				and cau				nit/4a408		
Denial of				service				43b0ef8:		
					•			daf70a47		
Service;				consum			-			5-NOV-
Cross Site				unspeci				a02b78c		•
Request		016-08-			nce: CV	E-2010		6073a4d		916/35
Forgery		25		4069			5		4	
		Hard	ware	; Oper	ating	Syste	m (H/	05)		
D-link										
Dir-8171	w) Firr	nware:	Dir-81	L8I(w) F	irmwai	e;Dir-	823 Fir	mware:	Dir-85	01;
Firmare;										
Firmwar										
The D-Li							(DIR-8	25) USE	s dua	l band
technolog					-					
allows yo										
simultane							-			
	Justy 5		ig ing						neuru	
CV Scoring	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Scoring Scale										
JLAIE										

5GHz band.					
			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	http://sup portannou ncement.u s.dlink.co m/announ cement/pu blication.a	H-OS-D-L-
Execute			a long session cookie.	spx?	DIR-8-
Code; Overflow	2016-08-25	9.3	Reference: CVE-2016- 5681	name=SA P10063	210916/35 5
Overnow	2010-00-23	9.5	2001	LT0002	J

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