National Critical Information Infrastructure Protection Centre											
NOIPE				CVE Re	•						
				Decem		16			Vo		No. 22
Vulnerability	Publish	CVSS	Descript	ion & CV	E ID		Pa	tch		NCII	PC ID
Type(s)	Date										
			Applic	cation (A	4)						
BMC											
Remedy Action	Request Syste	m									
BMC Remedy A	ction Request	System (A	ARS) is a j	proprieta	ry applic	ation	ser	ver dev	elop	ed init	tially by
Remedy Corp a	nd acquired by	BMC Soft	tware in 2	002.							
Denial of	21-12-2016	5	Remedy	AR Syster	n Server	in	NA	L		A-BM	IC-
Service;			BMC Ren	nedy 8.1 S	SP 2, 9.0,	9.0				REM	ED-
Execute Code;			SP 1, and	9.1 allow	rs attacke	ers				0301	16/01
Gain			to reset a	ırbitrary	password	ds					
Information			via a blank previous password. <b>REFERENCE: CVE-2016-2349</b>								
			REFERE	NCE: CVE	-2016-2	349					
NA	21-12-2016	5	Remedy	AR Syster	n Server	in	NA	L		A-BM	1C-
			BMC Ren	nedy 8.1 S	SP 2, 9.0,	9.0				REM	ED-
			SP 1, and	9.1 allow	rs attacke	ers				0301	16/02
			to reset a	rbitrary	password	ds					
			via a blar	nk previo	us passw	ord.					
			REFERE	NCE: CVE	-2016-2	349					
Bundler											
Bundler											
Bundler provid	es a consistent	environn	nent for Ri	uby proje	cts by tra	cking	ano	d installi	ing t	he exa	ct gems
and versions th	at are needed.										
NA	22-12-2016	7.5	Bundler	1.x might	allow		NA	<u>.</u>		A-BU	N-
			remote a	ttackers t	o inject					BUN	DL-
			arbitrary	Ruby co	de into ar	ı				0301	16/03
			applicati	on by leve	eraging a						
			gem nam	e collisio	n on a						
			secondar	y source.	NOTE: t	his					
			might ov	erlap CVE	E-2013-0	334.					
			REFERE	NCE: CVE	-2016-7	954					
Cisco											
Cloud-Center O	rchestrator										
Cisco Cloud-Cer	nter Orchestrat	or is a clo	ud-specifi	c multite	nant orch	<u>ne</u> stra	tior	tier.			
NA	26-12-2016	10	Vulnerab	ility in th	e Docker		htt	ps://too	ols.	A-CIS	S-
				onfigurati				co.com/		CLOU	JD-
				nter Orch				rity/cen		0301	16/04
			(CCO; for	merly Cli	Qr) could	d l		ontent/(			-
			-	unauther	-		-	Security			
			remote a	ttacker to	install			ory/ciso			
			Docker c	ontainers	with hig	h	sa-	·			
CV	1 10	0.0	2.4	4.5	F		,	7.0		0.0	0.40
Scoring	-1 1-2	2-3	3-4	4-5	5-6	6-7	/	7-8		8-9	9-10
Scale Scale											

Intercloud Fab			privilege system. This vult releases Orchestr deploym Docker I is open of bound to (any inte	75 0.0 <b>223</b>	20161 cco						
Intercloud Fab deployment mo							want t	to of	fer l	nybrid	l cloud
NA	26-12-2016	6.5	Vulneral Interclor and Cisc Provider unauthe attacker database products CSCus99 Releases	pility in Ci ad Fabric for o Interclor rs could al nticated, r to connect e used by to s. More Info 394. Know 37.3(0)ZN	sco for Busin ud Fabric low an remote t to the chese formation wn Affect I(0.99).	ess c for n:	https: cisco.c curity /conto coSect visory sa- 20161	com/s /cent ent/C urity/ v/cisc	se cer is Ad o-	A-CIS INTE 0301	
Jabber Guest											
Cisco Jabber Gu server operatin					=						
set up, managed								<b>J</b>			
NA	26-12-2016	6.4	Vulneral Jabber G allow an remote a connecti More Inf CSCvc31 Releases Fixed Re	oility in thuest Serve unauthen attacker to ons to arb formation: 635. Know 10.6(9). eleases: 11	e Cisco er could iticated, initiate oitrary ho wn Affect Known .0(0).	osts. ed	https: cisco.c curity /conto coSect visory sa- 20161 jabber	com/s /cent ent/C urity/ v/cisc	se cer is Ad o-	A-CIS JABBI 0301	
Dotcms											
Dotcms dotCMS is an Opopen standards Execute Code;		tent Man	Management System (CMS), built on leading Java technology and SQL injection vulnerability in https://githu A-DOT-								
SQL Injection			the REST API in dotCMS before				b.com	/dot(	CM	DOTO	CM-
CV Scoring Scale	-1 1-2	2-3	3-4 4-5 5-6					7-8	8	-9	9-10

			to execu comman paramet api/cont <b>REFERE</b>	ent/save/ NCE: CVE	ry SQL stName '1. - <b>2016-2</b> :	355	s/8	core/issu 3848			16/07
Execute Code; SQL Injection	19-12-2016	7.5	the REST 3.3.2 allo to execu comman paramet api/cont	ction vuln  I API in do  lows remote  te arbitran  ds via the  er to  cent/save/  NCE: CVE	otCMS beste attacked by SQL stName	fore ers	b.c S/c	ps://gith om/dot( core/issu 3848	CM	A-DO DOTO 0301	
Ffmpeg											
<i>Ffmpeg</i>	C	1.			1.0	,		1	,		
ffmpeg is a very									deo		
Denial of Service	23-12-2016	4.3	libavcod in FFmp remote a denial of huge me by the O file.	configure ec/aacded eg before attackers t f service (a mory, and S) via a cr	z_templat 3.2.1 allo to cause a allocatior l being ki afted MO	te.c ws a n of lled V	NA			A-FFI FFMF 0301	
Denial of Service	23-12-2016	4.3	The gsm libavcod FFmpeg remote a denial of via a cra	_parse fur ec/gsm_p before 3.1 attackers t f service (a fted AVI fi NCE: CVE	nction in arser.c in5 allows o cause aussert faule.	i S i ilt)	NA			A-FFI FFMF 0301	
Denial of Service	23-12-2016	4.3	libavfori FFmpeg remote a denial of used) via	l_gab2_sul mat/avide before 3.1 attackers t f service (I a a crafted <b>NCE: CVE</b>	c.c in 4 allows to cause a NULL poi AVI file.	s ı nter	NA			A-FFI FFMF 0301	
Denial of Service	23-12-2016	4.3	The avi_ libavfori FFmpeg remote a	read_seek nat/avide before 3.1 attackers t f service (a	function c.c in 4 allows to cause a	in S	NA			A-FFI FFMF 0301	
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8	3-9	9-10

	00.10.0015		via a crafted AVI file. <b>REFERENCE: CVE-20</b>		***			77.6
Denial of Service; Overflow	23-12-2016	4.3	The ff_draw_pc_font fin libavcodec/cga_dar FFmpeg before 3.1.4 remote attackers to cdenial of service (buf overflow) via a crafte <b>REFERENCE: CVE-20</b>	ta.c in allows ause a fer ed AVI file.	NA		A-FI FFM 030	
Gain Information	23-12-2016	4.3	The avi_read_header in libavformat/avided FFmpeg before 3.1.4 vulnerable to memor when decoding an AV has a crafted "strh" st REFERENCE: CVE-20	c.c in is y leak /I file that tructure.	NA		A-FI FFM 030	
NA	23-12-2016	6.8	The cavs_idct8_add_c in libavcodec/cavsds FFmpeg before 3.1.4 vulnerable to reading bounds memory whe decoding with cavs_d REFERENCE: CVE-20	p.c in is g out-of- en lecode.	NA		A-FI FFM 030	
NA	23-12-2016	6.8	The ff_log2_16bit_c full libavutil/intmath.h in before 3.1.4 is vulner reading out-of-bound memory when it decomalformed AIFF file. <b>REFERENCE: CVE-20</b>	n FFmpeg rable to ls odes a	NA		A-FI FFM 030	
NA	23-12-2016	4.3	The avi_read_nikon for libavformat/avidec.c FFmpeg before 3.1.4 vulnerable to infinite when it decodes an A that has a crafted 'not structure. REFERENCE: CVE-20	unction in in is loop VI file tg'	NA		A-FI FFM 030	
Denial of Service	23-12-2016	4.3	The zlib_refill function libavformat/swfdec.compression in the sum of the sum	c in allows cause an f service	NA		A-FI FFM 030	
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	23-12-2016	6.8	The raw_decode function in libavcodec/rawdec.c in FFmpeg before 3.1.2 allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted SWF file.  REFERENCE: CVE-2016-6671	NA	A-FFM- FFMPE- 030116/19
Google					
Chrome					
			ser developed by Google.		
Gain Information	17-12-2016	4.3	Google Chrome prior to 54.0.2840.85 for Android incorrectly handled rapid transition into and out of full screen mode, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages. REFERENCE: CVE-2016-5187	https://crbu g.com/63970 2	A-GOO- CHROM- 030116/20
Execute Code	17-12-2016	6.8	Devtools in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled objects after a tab crash, which allowed a remote attacker to perform an out of bounds memory read via crafted PDF files.  REFERENCE: CVE-2016-5186	https://crbu g.com/64496 3	A-G00- CHROM- 030116/21
Cross Site Scripting	17-12-2016	6.8	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly allowed reentrance of FrameView::updateLifecyclePh asesInternal(), which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.  REFERENCE: CVE-2016-5185		A-G00- CHROM- 030116/22
Cross Site	17-12-2016	6.8	PDFium in Google Chrome	https://crbu	A-GOO-
Scripting			prior to 54.0.2840.59 for	g.com/63065	CHROM-
CV Scoring Scale	-1 1-2	2-3	3-4 4-5 5-6 6	-7 7-8	8-9 9-10

			54.0.284 incorrect lifecycle CFFL_For rAnnot, remote a exploit h	ormFillter: which allo attacker to neap corru	android d object :KillFocu wed a o potentia	ally	4			0301	16/23
Execute Code; Overflow	17-12-2016	6.8	REFERE A heap u PDFium prior to Window 54.0.284 allows a potentia corrupti files.	PDF files. ENCE: CVE use after from Google 54.0.2840 us, Mac, and 10.85 for A use remote at ally exploit on via cra	ree in Chrome .59 for d Linux; android ctacker to heap fted PDF	,	me oo m, sta ch	tps://chrereleases gleblog.c /2016/10 able- annel- date-for- sktop.htr	s.g so 0/	A-GO CHRO 0301	
Overflow	17-12-2016	6.8	Blink in to 54.0.2 Mac, and for Andr validation which al attacker heap con HTML p	Google Ch 2840.59 fo d Linux; 54 roid had in on in bitma lowed a ro to potent cruption v ages.	rome pri r Windov 4.0.2840. sufficien ap handli emote ially expl ia craftec	or ws, 85 t ng, oit	me oo m, sta ch up	tps://chrereleases gleblog.c /2016/10 able- annel- date-for- sktop.htr	s.g so 0/	A-GO CHRO 0301	
Cross Site Scripting	17-12-2016	4.3	heap corruption via crafted HTML pages.  REFERENCE: CVE-2016-5182  Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted execution of v8 microtasks while the DOM was in an inconsistent state, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages.  REFERENCE: CVE-2016-5181					tps://crb		A-GO CHRO 0301	
Bypass	17-12-2016	4.3	Google ( for iOS h	Chrome properties and insufficient of URLs	ior to 54. cient			tps://crb com/639		A-GO CHRO 0301	
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-	7	7-8		8-9	9-10

			. ,	1	DOM 1	. ,					
			windows allowed a bypass resulting navigation schemes w	remote a striction n to certa	attacker s on ain URL						
			pages. <b>REFEREN</b>			193					
Bypass	17-12-2016	4.3	Blink in Goto 54.0.28 missed a Goto redirect in which allocattacker to restriction pages.  REFEREN	440.59 fo CORS che n TextTra owed a re o bypass ns via cra	r Windoveck on ackLoadeemote cross-or	ws er, rigin ML		ps://crb om/633		A-GO CHRO 0301	
Cross Site Scripting	17-12-2016	4.3	Bookmark Chrome p for Windo 54.0.2840 insufficier supplied of remote at arbitrary s (UXSS) via pages, as of interpreta userinfo a http://jav mple.com REFEREN	rior to 5- ows, Mac 0.85 for A nt validat data, whi tacker to scripts o a crafted demonst ation con and scher vascript: URL.	4.0.2840, and Lindroid he tion of ch allower inject r HTML rated by flict between an oayload@	.59 ux; aad ed a an veen		ps://crb om/639		A-GO CHRO 0301	
NA	17-12-2016	6.8	Google Ch 54.0.2840 Mac, and I for Andro handled o during sho allowed a perform a memory r HTML pag REFEREN	rome pr 0.59 for V Linux; 54 id incorr bject life utdown, remote a n out of read via o	ior to Vindows, 4.0.2840.3 ectly ecycles which attacker to bounds crafted	, 85 to		ps://crb om/642		A-GO CHRO 0301	
NA	17-12-2016	4.3	Google Ch 54.0.2840 Mac, and I	rome pr 0.59 for V	ior to Vindows,	,		ps://crb om/646		A-GO CHRO 0301	
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8	8-9	9-10

				C- A 1								
					oid permi		. 1					
				_	on to blob							
					onical orig							
					a remote a		to					
				_	e contents		C. 1					
					x (URL baı	') via crai	tted					
				HTML p								
					NCE: CVE		189	_				_
NA	17	-12-2016	4.3	_	issues in				ps://crb		A-GO	
				_	Chrome pr			_	om/565	76	CHRO	
					10.59 for V			0			0301	16/32
					l Linux all							
					to spoof v	•	arts					
					ser UI via o	crafted						
				HTML p	_							
					NCE: CVE		188					
NA	17	-12-2016	4.3		Chrome pr				ps://crb		A-GO	
					10.85 for A			_	om/639	70	CHRO	
					tly handle	_		2			0301	16/33
					n into and							
					node, whic							
					attacker to	_						
					of the On	•						
				_	crafted H7							
					NCE: CVE							
NA	17	-12-2016	6.8		s in Google		!		ps://crb		A-GO	
				_	54.0.2840			_	om/644	96	CHRO	
					rs, Mac, an	•		3			0301	16/34
					0.85 for A							
					tly handle	-	;					
					ab crash, v							
					a remote		to					
				-	an out of							
				-	read via o	rafted PI	)F					
				files.								
		40.0011			NCE: CVE			,	., -		4 6 6	0
NA	17	-12-2016	6.8		Google Ch	•			ps://crb		A-GO	
					2840.59 fo		,	_	om/621	36	CHRO	
					l Linux; 54		85	0			0301	16/35
					oid incorr	•						
				allowed reentrance of								
					iew::updat							
					rnal(), wh							
					attacker							
				an out o	f bounds n	nemory r	ead					
CV	0-1	1-2	2-3	3-4	4-5	5-6	6-'	7	7-8		8-9	9-10
Scoring	0-1	1-2	2-3	3-4 4-5 5-6 6				′	7-0		3 <b>-3</b>	<del>9-1</del> 0
Scale												

			via crafted HTML pages. <b>REFERENCE: CVE-2016-5185</b>		
NA	17-12-2016	6.8	PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles in CFFL_FormFillter::KillFocusForAnnot, which allowed a remote attacker to potentially exploit heap corruption via crafted PDF files.  REFERENCE: CVE-2016-5184	https://crbu g.com/63065 4	A-G00- CHROM- 030116/36
NA	17-12-2016	6.8	A heap use after free in PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android allows a remote attacker to potentially exploit heap corruption via crafted PDF files.  REFERENCE: CVE-2016-5183	https://chro mereleases.g oogleblog.co m/2016/10/ stable- channel- update-for- desktop.html	A-GOO- CHROM- 030116/37
Overflow	17-12-2016	6.8	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation in bitmap handling, which allowed a remote attacker to potentially exploit heap corruption via crafted HTML pages.  REFERENCE: CVE-2016-5182	https://chro mereleases.g oogleblog.co m/2016/10/ stable- channel- update-for- desktop.html	A-GOO- CHROM- 030116/38
Cross Site Scripting	17-12-2016	4.3	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted execution of v8 microtasks while the DOM was in an inconsistent state, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages.	https://crbu g.com/64521 1	A-G00- CHROM- 030116/39
CV Scoring Scale	0-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10

			<b>REFERENCE: CVE-2016-5181</b>							
Horde										
Groupware										
Horde Groupwa	ire is a free, ent	erprise r	eady, browser based collaboratio	n suite.						
Cross Site Scripting	20-12-2016	4.3	Cross-site scripting (XSS) vulnerability in the Horde Text Filter API in Horde Groupware and Horde Groupware Webmail Edition before 5.2.16 allows remote attackers to inject arbitrary web script or HTML via crafted data:text/html content in a form (1) action or (2) xlink attribute. REFERENCE: CVE-2016-5303	NA	A-HOR- GROUP- 030116/40					
Image-info Pr	oject									
Image-info For	Perl									
Denial of Service	22-12-2016	5.8	perl-Image-Info: When parsing an SVG file, external entity expansion (XXE) was not disabled. An attacker could craft an SVG file which, when processed by an application using perl-Image-Info, could cause denial of service or, potentially, information disclosure.  REFERENCE: CVE-2016-9181	NA	A-IMA- IMAGE- 030116/41					
Imagemagick										
<b>Imagemagick</b>	C		.1							
Execute Code	a software suit 23-12-2016	6.8	An exploitable out of bounds write exists in the handling of compressed TIFF images in ImageMagicks's convert utility. A crafted TIFF document can lead to an out of bounds write which in particular circumstances could be leveraged into remote code execution. The vulnerability can be triggered through any	ap images. NA	A-IMA- IMAGE- 030116/42					
CV Scoring Scale	Scoring   0-1   1-2   2-3   3-4   4-5   5-6   6-7   7-8   8-9   9-10									

			user conti	y this fu	ty.						
Joomla			REFEREN	CE: CVE	-2016-8	707					
Joomla!											
Joomla! is the m	nobile-ready and	d user-fr	endly way	to build	vour wel	bsite.					
NA NA	16-12-2016	5	An issue very component ls/registration before 3.6 of registration to gain accuser's accuser's grousername demonstration that 'registration' registration' registration of the component of the c	vas disconts/come ation.phy o.5. Incornation for the sessing error encess to a ount and up mappy and pass ated by stargets ton.regis	overed in users/me in Joom rect filter me data on on a nables a uregistered reset the bings, ssword, as submitting the ter`task.	aode ala! ring user ed e	.joc nnc ts/ nev joo 5-	ps://ww omla.org ounceme release- vs/5693 mla-3-6	s/a en 3-	A-J00 J00M 0301	
NA	16-12-2016	5	demonstrated by submitting a form that targets the 'registration.register' task.  REFERENCE: CVE-2016-9838  An issue was discovered in templates/beez3/html/com_c ontent/article/default.php in Joomla! before 3.6.5.  Inadequate permissions checks in the Beez3 layout override of the com_content article view allow users to view articles that should not be publicly accessible, as demonstrated by an index.php?option=com_content t&view=article&id=1&templat e=beez3 request.				.joc nnc ts/ nev joo 5-	ps://ww omla.org ounceme release- vs/5693 mla-3-6	s/a en 3-	A-J00 J00M 03012	
KDE			REFEREN						ı		
Kmail											
KMail is the em	ail component o	of Kontac	t, the integ	rated pe	rsonal in	forma	tion	manage	er fro	m KD	E.
Execute Code	23-12-2016	7.5	KMail since version 5.3.0 used a QWebEngine based viewer that had JavaScript enabled. HTML Mail contents were not sanitized for JavaScript and included code was executed.				NA			A-KDI KMAI	E-
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-	-9	9-10

				REFERE	NCE: CVE	-2016-7	968			
NA	23-	12-2016	5.8	a QWebl that had Since the executed security access to URLs wa	nce versio Engine bas JavaScrip e generate d in the loc context by o remote a as enabled	sed viewe t enabled d html is cal file y default nd local	er I.	NA	A-KI KMA 0302	
Lynx				•					<u> </u>	
Lynx Lynx is a hi terminals.	ghly cor	nfigurable	text-bas	ed web b	rowser fo	r use on	cursor	-addressa	ble chara	cter cell
NA	22-	12-2016	5	doesn't p compon correctly part end instead l connecti	vas found parse the a ent of the y when the s with '?', be tricked ing to a dif	authority URL host nat and could into ferent ho	me d	NA	A-LY LYN 0302	
Microsoft										
.net Framev .NET Frame primarily or	work (p			t) is a sof	ftware fran	nework	develo	oed by Mi	crosoft tl	nat runs
Bypass; Gair Information	n 20-	12-2016	5	The Data Provider for SQL Server in Microsoft .NET Framework 4.6.2 mishandles a developer-supplied key, which allows remote attackers to bypass the Always Encrypted protection mechanism and obtain sensitive cleartext information by leveraging key guessability, aka ".NET Information Disclosure Vulnerability." REFERENCE: CVE-2016-7270						ICNET 116/48
Auto Update Download, customers -	Install o	or Update	Microso	oft AutoUp	odate (Mac	:) - Prov	vides la	itest MS (	Office up	dates to
Gain Privileges	20-	12-2016	4.6		ed search poility in Mi			NA	A-Mi AUT	
CV Scoring	0-1	1-2	2-3	3-4 4-5 5-6 6-7 7-8						9-10

Scale

			Updater for Mac allows local users to gain privileges via a Trojan horse executable file, aka "Microsoft (MAU) Office Elevation of Privilege Vulnerability."  REFERENCE: CVE-2016-7300			a e, e			03	0116/49
Edge	wasaft Edga tha	all marry	h.w.o.v.o.o.w 6	ou havina	a hattan	ah a				
Experience Mic Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	The scri Microso attacker code or service ( via a cra "Scriptin Corrupti different CVE-201 7288, an	pting engi ft Edge all s to execu cause a de memory of fted web s ig Engine ion Vulnerab t vulnerab 6-7286, C	nes in ow remo te arbitra enial of corruptio site, aka Memory rability," cility than EVE-2016	te ary n) a	NA		ED	MIC- GE- 0116/50
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	The scri Microso attacker code or service ( via a cra "Scriptir Corrupti different CVE-201 7288, ar	pting engift Edge all s to executause a defined web song Engine toulners to	nes in ow remo te arbitra enial of corruptio site, aka Memory rability," dility than EVE-2016	te ary n) a	NA		ED	MIC- GE- 0116/51
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	The scri Microso attacker code or service ( via a cra "Scriptir Corrupti different CVE-201 7296, ar	pting engift Edge all s to execu cause a de memory of the fed web so generated with the fed with the fed to th	nes in ow remo te arbitra enial of corruptio site, aka Memory rability," cility than EVE-2016	te ary n) a	NA		ED	MIC- GE- 0116/52
CV Scoring Scale	-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	20-12-2016	7.6	The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7288, CVE-2016-7296, and CVE-2016-7297.  REFERENCE: CVE-2016-7286	NA	A-MIC- EDGE- 030116/53
Cross Site Scripting	20-12-2016	4.3	Cross-site scripting (XSS) vulnerability in Microsoft Edge allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Edge Information Disclosure Vulnerability," a different vulnerability than CVE-2016- 7206. REFERENCE: CVE-2016-7280	NA	A-MIC- EDGE- 030116/54
Cross Site Scripting	20-12-2016	4.3	Cross-site scripting (XSS) vulnerability in Microsoft Edge allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Edge Information Disclosure Vulnerability," a different vulnerability than CVE-2016- 7280. REFERENCE: CVE-2016-7206	NA	A-MIC- EDGE- 030116/55
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	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." REFERENCE: CVE-2016-7181	NA	A-MIC- EDGE- 030116/56

Edge;Internet Explorer

Experience Microsoft Edge, the all new browser for having a better web experience; Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft and included as part of the

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

Microsoft Windows line of operating systems, starting in 1995.										
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	The scripting engines in Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." REFERENCE: CVE-2016-7287	NA	A-MIC- EDGE;- 030116/57					
Cross Site Scripting	20-12-2016	4.3	Cross-site scripting (XSS) vulnerability in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Browser Information Disclosure Vulnerability." REFERENCE: CVE-2016-7282	NA	A-MIC- EDGE;- 030116/58					
Bypass	20-12-2016	2.6	The Web Workers implementation in Microsoft Internet Explorer 10 and 11 and Microsoft Edge allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Microsoft Browser Security Feature Bypass Vulnerability." REFERENCE: CVE-2016-7281	NA	A-MIC- EDGE;- 030116/59					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." REFERENCE: CVE-2016-7279	NA	A-MIC- EDGE;- 030116/60					
<b>Excel</b> Microsoft Excel	is a spreadshee	t develo	ped by Microsoft for Windows, ma	acOS, Android a	nd iOS.					
CV										

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

Execute Code; Bypass	20-12-2016	4.3	2013 SP 2016 mi which m remote a arbitrary documen Office Se Vulneral	ft Excel 20 1, 2013 RT sparses fil akes it eas attackers t y code via nt, aka "Mi curity Fea pility." NCE: CVE	SP1, and e format sier for o execute a crafted crosoft ture Byp	d s, e ass	NA		E	A-MIC- EXCEL- 930116/	61
Excel For Mac											
Microsoft Excel	better than eve	r for Ma	c, and mu	ch more p	rograms.						
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	9.3	and Exceremote a arbitrary denial of corrupti document Office M	ft Excel for attackers to code or confervice (ron) via a confermation emory Confermation coility."	Mac allo o execute ause a nemory rafted crosoft ruption	ow e	NA		E	A-MIC- EXCEL- 030116/	62
Microsoft Excel Microsoft Excel user to open, v Microsoft Office earlier versions	better than ever iew and print Me Compatibility	er for M MS Excel	ac, and m	uch more hout insta	progran lling Mic	ns; The crosoft	e Fr Exc	ee Exce cel on h	l View iis or	ver allov her syst	vs a em;
Execute Code; Bypass	20-12-2016	6.8	Excel 20 SP1, Exc 2016, Of Pack SP3 Excel 20 a registr user-ass to execu comman embedd documer Office Se Vulneral	ft Excel 20 10 SP2, Exel 2013 R fice Comp 3, Excel Vio 16 for Mac y check, w isted remo te arbitran ds via crai ed content nt, aka "Mi ecurity Fea pility." NCE: CVE	ccel 2013 SP1, Exatibility ewer, and mishan hich allo ote attack fy fted in a crosoft ture Byp	cel d dle ws cers	NA		E	A-MIC- EXCEL- 030116/	63
Denial of Service; Gain	20-12-2016	5.8		ft Excel 20 Impatibilit	•		NA			A-MIC- EXCEL-	
CV	-1 1-2	2-3	3-4	4-5	5-6	6-7	,	7-8	8-9		9-10

Scale

Information    Excel Viewer, Excel for Mac 2011, and Excel 2016 for Mac allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability."    Execute Code;   20-12-2016   6.8   Microsoft Excel 2007 SP3,   Excel 2013 RT SP1, Excel 2014 RT SP1, Excel 2015 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that its mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."    Excel, Excel Viewer, Office Compatibility Pack, SP1, Excel 2016 RT Server Moss) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.   Denial of Service; Gain Information   SP2, Excel 2013 RT SP1, Excel 2013 RT SP1, Excel 2016 RT SP1, Excel 2016 RT SP2, Excel 2013 SP1, Excel 2017 SP2, allow remote attackers to obtain sensitive information   From Process memory or cause a denial of service on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information   From Process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability."	Information			Errael 17	тигом Г	l for Mr.	, 1			0.0	00116764
allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability."  Execute Code; Bypass  Execute C	information									03	0116/64
obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability."  REFERENCE: CVE-2016-7264  Execute Code; Bypass  Execute Code; Bypass  Execute Code; Bypass  6.8 Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2013 SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability." REFERENCE: CVE-2016-7262  Excel, Excel Viewer; Office Compatibility Pack; Sharepoint Server Microsoft Excel is a spreadsheet developed by Microsoft of Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collobartively creating, managing and sharing documents and Web services.  Denial of 20-12-2016 S.8 Microsoft Excel 2007 SP3, Excel 2013 RTSP1, Excel 2013 RTSP1				•			iac				
Execute Code; Bypass							_				
a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability."  REFERENCE: CVE-2016-7264  Execute Code; Bypass  8 20-12-2016 Bypass  8 Microsoft Excel 2007 SP3, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2013 SP1, Excel 2016 SP2, Excel 2013 SP1, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 20											
Execute Code; Bypass  Execute Compatibility Pack SP3, and Exect Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability." REFERENCE: CVE-2016-7262  Exect, Exect Viewer; Office Compatibility Pack, Sharepoint Server Microsoft Exect Is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Exect Viewer allows a user to open, view and print MS Exect files without installing Microsoft Exect on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal- based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Exect Code; Exect Viewer, Exect Services and Exect Every (Most) is the full version of a portal- based platform for collaboratively creating, managing and sharing documents and Web services.  Exect Every (Microsoft Exect Every (Most) is the full version of a portal- based platform for collaboratively creating, managing and sharing documents and Web services.  Exect Every (Microsoft Exect Every				_		-	ause				
Execute Code;   20-12-2016   6.8   Microsoft Excel 2007 SP3,   Excel 2013 RT SP1, Excel 2013 RT SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility   Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."   REFERENCE: CVE-2016-7262   Excel Viewer; Office Compatibility Pack; Sharepoint Server Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services. Denial of 20-12-2016   5.8   Microsoft Excel 2007 SP3, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack; SP3, Excel 2018 RT SP1, Excel 2016 Greece and Web services.   Services on SharePoint Server 2010 SP2, and Excel 2016 Greece and Web services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Uniforosoft Control of Disclosure"   Wicrosoft Control of Disclosure   W						•					
Execute Code; Bypass  Execute Compatibility Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."  Execute Code; Bypass  Execute Viewer; Office Compatibility Pack, Sharepoint Server  Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Service; Gain Information  Excel 2010 SP2, Excel 2013 SP1, Exce					-						
Execute Code; Bypass    20-12-2016											
Execute Code; Bypass    Secol 20-12-2016   6.8   Microsoft Excel 2007 SP3,						i Disclosu	ire				
Execute Code; Bypass  20-12-2016 Bypass  20-12-2016 Bypass  8 Microsoft Excel 2007 SP3, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability." REFERENCE: CVE-2016-7262  Excel, Excel Viewer; Office Compatibility Pack; Sharepoint Server Microsoft Excel viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal- based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Service; Gain Information  Service; Gain Information  Service; Gain Service				Vulneral	oility."						
Bypass   Excel 2010 SP2, Excel 2013   SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."   REFERENCE: CVE-2016-7262    Excel; Excel Viewer; Office Compatibility Pack; Sharepoint Server Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of 20-12-2016   5.8				REFERE	NCE: CVE	-2016-72	264				
SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."  REFERENCE: CVE-2016-7262  Excel, Excel Viewer; Office Compatibility Pack, Sharepoint Server  Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of 20-12-2016 5.8 Microsoft Excel 2007 SP3, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure	Execute Code;	20-12-2016	6.8	Microso	ft Excel 20	07 SP3,		NA		A-	MIC-
2016, Office Compatibility Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability." REFERENCE: CVE-2016-7262  Excel; Excel Viewer; Office Compatibility Pack; Sharepoint Server Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal- based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Service; Gain Information  5.8  Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2016 Services on SharePoint Server 2007 SP3, and Excel	Bypass			Excel 20	10 SP2, Ex	xcel 2013	}			ЕΣ	KCEL-
2016, Office Compatibility Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability." REFERENCE: CVE-2016-7262  Excel; Excel Viewer; Office Compatibility Pack; Sharepoint Server Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal- based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Service; Gain Information  5.8  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, and Excel Services on SharePoint Server 2007 SP3, an				SP1, Exc	el 2013 R'	T SP1, Ex	cel			03	80116/65
Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."  REFERENCE: CVE-2016-7262  Excel;Excel Viewer;Office Compatibility Pack;Sharepoint Server  Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of 20-12-2016 S.8 Microsoft Excel 2007 SP3, Excel 2013 SP1, Excel 2013 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure											,
allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."  **REFERENCE: CVE-2016-7262**  **Excel; Excel Viewer; Office Compatibility Pack; Sharepoint Server**  Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of 20-12-2016					_						
attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."  REFERENCE: CVE-2016-7262  Excel;Excel Viewer;Office Compatibility Pack,Sharepoint Server  Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of 20-12-2016					•		l l				
commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."  REFERENCE: CVE-2016-7262  Excel;Excel Viewer;Office Compatibility Pack;Sharepoint Server  Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Service; Gain Information  Service; Gain Sp1, Excel 2013 Sp2, Excel 2013 Sp1, Excel 2013 Sp1, Excel 2013 RT Sp1, Excel 2016, Office Compatibility Pack Sp3, Excel Viewer, Excel Services on SharePoint Server 2007 Sp3, and Excel Services on SharePoint Server 2010 Sp2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure"											
that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability."  REFERENCE: CVE-2016-7262  Excel;Excel Viewer;Office Compatibility Pack;Sharepoint Server  Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Service; Gain Information  SP1, Excel 2013 RT SP1, Excel 2013 SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure"							-				
click, aka "Microsoft Office Security Feature Bypass Vulnerability." REFERENCE: CVE-2016-7262  Excel;Excel Viewer;Office Compatibility Pack;Sharepoint Server Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Service; Gain Information  SP1, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP2, allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure							1				
Security Feature Bypass   Vulnerability."   REFERENCE: CVE-2016-7262						•					
Excel; Excel Viewer; Office Compatibility Pack; Sharepoint Server  Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Service; Gain Information  5.8 Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2010 SP2, Excel 2013 SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure											
REFERENCE: CVE-2016-7262  Excel;Excel Viewer;Office Compatibility Pack;Sharepoint Server  Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Service; Gain Information  Service; Gain Information  Service; Gain Information  Service 2010 SP2, Excel 2013 SP1, Excel 2013 SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure						ypass					
Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of 20-12-2016						2016 7	262				
Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of 20-12-2016	F1 F117	O.C C					202				
Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of Service; Gain Information			•		-			(	C 4 . J		J :OC Th
Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.  Denial of 20-12-2016		-		_							
Denial of 20-12-2016 5.8 Microsoft Excel 2007 SP3, NA A-MIC- Service; Gain Information SP1, Excel 2013 SP1, Excel 2013 SP1, Excel 2013 SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure"											
Denial of Service; Gain Information  20-12-2016  Service; Gain Information  5.8  Microsoft Excel 2017 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, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure											
Service; Gain Information  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, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure							locum		ana we		
Information  SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure		20-12-2016	5.8			•		NA			
2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure											
Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure	Information						cel			03	80116/66
Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure				•							
2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure				Pack SP3	B, Excel Vi	ewer, Exc	cel				
on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure				Services	on Sharel	Point Ser	ver				
allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure				2007 SP	3, and Exc	el Servic	es				
obtain sensitive information from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure				on Share	Point Ser	ver 2010	SP2				
from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure				allow re	mote atta	ckers to					
from process memory or cause a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure							n				
a denial of service (out-of- bounds read) via a crafted document, aka "Microsoft Office Information Disclosure											
bounds read) via a crafted document, aka "Microsoft Office Information Disclosure				•		•					
document, aka "Microsoft Office Information Disclosure						•					
Office Information Disclosure					-						
							ire				
† MILLOL MALLET Y						Disclosu					
CV	CV										
Scoring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Λ_	1-2	2-3	3-4	4-5	5-6	6-7		7-8	8-9	9-10
Scale Scale Scale	<u> </u>										

				REFERE	NCE: CVE	-2016-72	265				
Internet Exploi	rer									•	
Internet Explor	er is	a discontin	ued seri	es of grap	hical web	browser	s dev	elop	ed by Mi	icrosof	t and
included as par	t of t	he Microso	ft Windo	ws line of	f operating	g systems	s, star	ting	g in 1995		
Gain	20-	12-2016	4.3	Microso	ft Internet	Explore	r 10	NA	1	A-	·MIC-
Information				and 11 a	llows rem	ote				IN	ITER-
				attacker	s to obtair	ı sensitiv	e			03	30116/67
				information from process							
				memory	via a craf	ted web s	site,				
				aka "Inte	ernet Expl	orer					
				Informa	tion Disclo	sure					
				Vulneral	oility."						
				REFERE	NCE: CVE	-2016-72	284				
Denial of	20-	12-2016	9.3	Microso	ft Internet	Explore	r 9	NA	Α	A-	MIC-
Service;					11 allows					IN	ITER-
Execute Code;				attacker	s to execu	te arbitra	ary			03	30116/68
Overflow;				code or	cause a de	nial of					
Memory				service (	memory o	corruptio	n)				
Corruption				via a cra	fted web s	ite, aka					
				"Interne	t Explorer	Memory	7				
					on Vulner						
				REFERE	NCE: CVE	-2016-72	283				
Gain	20-	12-2016	2.6		ft Internet	-	r 9	NA	Α		·MIC-
Information					11 allows						ITER-
					s to obtair		e			03	30116/69
					tion from <sub>J</sub>						
					via a craf		site,				
					ndows Hyp						
					ibrary Info						
					re Vulnera						
- 40				REFERE	NCE: CVE	-2016-72	278				
Office Microsoft Office	is ai	n office suit	te of ann	lications	servers ai	nd servic	es de	velo	ned by M	licroso	ıft
Denial of		12-2016	9.3		ft Office 20			N/	•		MIC-
Service;					attackers t						FFIC-
Execute Code;					y code or o						30116/70
Overflow;					f service (1						,
Memory					on) via a c						
Corruption					nt, aka "Mi						
•					emory Coi						
				Vulnerability."							
					NCE: CVE	-2016-72	<u> 27</u> 7				
Gain	20-	12-2016	7.2	Microso	ft Office 20	)10 SP2,		NA	1	A-	·MIC-
Privileges				2013 SP	1, 2013 RT	ΓSP1, an	d			0	FFIC-
					shandles l					03	30116/71
CV Scoring Scale	-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

		loading, which allows local
		users to gain privileges via a
		crafted application, aka
		"Microsoft Office OLE DLL Side
		Loading Vulnerability."
		REFERENCE: CVE-2016-7275
OCC OCC C CITIE D	1 0 CC	TAY I A CI CO TAY I TAY I A

## Office;Office Compatibility Pack;Office Web Apps;Sharepoint Server;Word;Word Automation Services;Word For Mac

Microsoft Office is an office suite of applications, servers, and services developed by Microsoft; Microsoft Office Compatibility Pack makes files created with Office 2007 and later work seamlessly on earlier versions of Office; Office Online (previously Office Web Apps) is an online office suite offered by Microsoft, which allows users to create and edit files using lightweight, web browser-based versions of Microsoft Office applications: Word, Excel, PowerPoint and OneNote; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services; Microsoft Word is a word processor developed by Microsoft; Word Automation Services is a new SharePoint Server 2010 technology that enables unattended, server-side conversion of documents that are supported by Microsoft Word; Made with Mac in mind, Office 2016 for Mac gives you access to your favorite Office applications - anywhere, anytime and with anyone-includes new versions of Word, Excel PowerPoint, Outlook, and OneNote.

			, Excel, Power Pollit, Outlook, and		
Denial of	20-12-2016	5.8	Microsoft Word 2007 SP3,	NA	A-MIC-
Service; Gain			Office 2010 SP2, Word 2010		OFFIC-
Information			SP2, Office Compatibility Pack		030116/72
			SP3, Word for Mac 2011, Word		
			Automation Services on		
			SharePoint Server 2010 SP2,		
			and Office Web Apps 2010 SP2		
			allow remote attackers to		
			obtain sensitive information		
			from process memory or cause		
			a denial of service (out-of-		
			bounds read) via a crafted		
			document, aka "Microsoft		
			Office Information Disclosure		
			Vulnerability," a different		
			vulnerability than CVE-2016-		
			7290.		
			REFERENCE: CVE-2016-7291		
Denial of	20-12-2016	5.8	Microsoft Word 2007 SP3,	NA	A-MIC-
Service; Gain			Office 2010 SP2, Word 2010		OFFIC-
Information			SP2, Office Compatibility Pack		030116/73
			SP3, Word for Mac 2011, Word		,
			Automation Services on		
			SharePoint Server 2010 SP2,		
			and Office Web Apps 2010 SP2		
			allow remote attackers to		
	I				

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

Г	T			ı					
			obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability," a different vulnerability than CVE-2016-7291.  REFERENCE: CVE-2016-7290						
Denial of Service; Gain Information	20-12-2016	5.8	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Office Compatibility Pack SP3, Word Viewer, Word for Mac 2011, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability." REFERENCE: CVE-2016-7268	NA	A-MIC- OFFIC- 030116/74				
	is an office suit		lications, servers, and services de Office 365 subscription and as a or	•					
Denial of 20-12-2016									
Office; Word Viewer  Microsoft Office is an office suite of applications, servers, and services developed by Microsoft;  Microsoft Word Viewer is a freeware program for Microsoft Windows that can display and print									

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

Microsoft Word	documents.										
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	9.3	Office 20 Office for 2016 for attacker code or service ( via a cra "Microso Corrupti	ft Office 20 010 SP2, War Mac 201 Mac allows to execucause a de memory of fted document Office Mace NCE: CVE	Vord Viev 1, and Of w remote te arbitra nial of corruptio ment, aka Memory rability."	fice ary n)	NA			A-MI OFFI 0301	
Publisher	-h	11	al-t-a-a-a-a-a	.l: _l. :		C	1/1:	C+			
Microsoft Public Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	9.3	Microso allows re execute cause a c (memor crafted c "Microso Corrupti	ft Published arbitrary of denial of some corruption of the comment, of the comment of the	er 2010 S ackers to code or ervice on) via a aka Memory ability."	P2	NA			A-MI PUBI 0301	
Netapp											
<b>Snap Creator F</b> OS-independen third-party app	t Snap Creator	Framew	ork integ	rates NetA	App data	prote	ectio	on with	a b	road r	ange of
Gain Information	21-12-2016	5	Framew disclose which co unautho	Snap Crea ork before s sensitive ould be vie rized user NCE: CVE	e 4.3.1 e informa ewed by a	ın	NA	1		A-NE SNAF 0301	
Nvidia			TIEL ELLE								
Geforce Experior Redesigned from gaming rig upda	m the ground up				the new (	GeFor	ce I	Experien	ce k	eeps y	our
Directory Traversal	16-12-2016	5	NVIDIA 3.x before contains NVIDIA a local w /Visual(	GeForce E re GFE 3.1 a vulnera Web Help yeb API en DPS/v.1.0.,	.0.52 ability in er.exe wh dpoint, /, lacks		.cu /a <sub>]</sub> s/o	p://nvid sthelp.co pp/answ detail/a_ 279	om ver	A-NV GEFO 0301	
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8		8-9	9-10

			for infor a directo	er validat mation dis ory travers	sclosure v sal attack	via					
Con Duines			REFERE	NCE: CVE	-2016-88	827					
<b>Gpu Driver</b> NVIDIA GPUs d	rive a visually st	unning.	premium	experienc	e on desl	kton a	nd r	noteboo	k P(	ls.	
Denial of Service	16-12-2016	4.9	All versi Display vulneral mode lay Window Linux) w a GPU in to a deni	ons of NVI Driver con Dility in the yer (nvldd rs or nvidia where a use terrupt st ial of servi	DIA GPU atain a e kernel mkm.sys a.ko for er can can orm, lead ce.	for use ling	htt .cus /ap	p://nvid sthelp.co pp/answ letail/a_	lia om er	A-NV D-	I-GPU 16/80
Denial of Service; Overflow	16-12-2016	7.2	All versi Window contain a kernel m (nvlddm DxgDdiF of an inp validated service of	ons of NVI as GPU Dis a vulnerab node layer akm.sys) h ascape who out buffer d, leading or potentia	DIA play Driv pility in the andler fo ere the si is not to denial	er ne r ze of	.cus	p://nvid sthelp.co pp/answ letail/a_ 278	om er	D-	T-GPU 16/81
NA	16-12-2016	7.2	Window contain a kernel m (nvlddm DxgDdiF access couser to vergistry privilege to escala REFERE	ons of NVI ons GPU Dis a vulnerat node layer lkm.sys) h scape whe ontrols all vrite a par intended t ed users of ation of pri	play Drivolity in the andler foere improperson a regular of the form ivileges2016-83	r oper ular	.cus /ap	p://nvid sthelp.co pp/answ letail/a_ 278	om er	D- 0301	I-GPU 16/82
Denial of Service; Overflow	16-12-2016	7.2	Window contain a kernel m DxgDdiE of an inp	ons of NVI is GPU Dis a vulnerat node layer Escape who out buffer d leading t	play Driv bility in th handler ere the si is not	ne for ze	.cus /ap	p://nvid sthelp.co pp/answ letail/a_ 278	om er	D-	I-GPU 16/83
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	,	7-8	8	8-9	9-10

CV			(IIVIddiiikiii.5y5) Ildiidici 101	/ 1237	
Denial of Service	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for	http://nvidia .custhelp.com /app/answer s/detail/a_id /4257	A-NVI-GPU D- 030116/87
			kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where a check on a function return value is missing, potentially allowing an uninitialized value to be used as the source of a strcpy() call, leading to denial of service or information disclosure. REFERENCE: CVE-2016-8820	s/detail/a_id /4257	
Denial of Service	16-12-2016	5.6	access controls may allow a user to access arbitrary physical memory, leading to an escalation of privileges.  REFERENCE: CVE-2016-8821  All versions of NVIDIA  Windows GPU Display Driver contain a vulnerability in the	http://nvidia .custhelp.com /app/answer	A-NVI-GPU D- 030116/86
NA	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer handler for DxgDdiEscape where improper	http://nvidia .custhelp.com /app/answer s/detail/a_id /4278	A-NVI-GPU D- 030116/85
Denial of Service	16-12-2016	7.2	service or possible escalation of privileges  REFERENCE: CVE-2016-8823  All versions of NVIDIA  Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x600000E, 0x600000F, and 0x6000010 where a value passed from a user to the driver is used without validation as the index to an internal array, leading to denial of service or potential escalation of privileges.  REFERENCE: CVE-2016-8822	http://nvidia .custhelp.com /app/answer s/detail/a_id /4278	A-NVI-GPU D- 030116/84

			_	Escape w							
				o a kernel		ay					
				ned to the	•						
			_	o possible		f					
			service o	or escalati	on of						
			privilege	es.							
				NCE: CVE	-2016-8	819					
Denial of	16-12-2016	7.2	All versi	ons of NV	IDIA		htt	tp://nvid	lia	A-NV	'I-GPU
Service			Window	s GPU Dis	play cont	ain		isthelp.co		D-	
				ability in				pp/answ		0301	16/88
				zer (nvldo				detail/a_		0001	10,00
				for DxgDo	•	,	•	257			
				pointer p	•	m a	/ 1	207			
				he driver		III a					
				validatior		to					
					_						
				service o	•	dl					
				n of privi	_	040					
Daniel - C	16 12 2016	7.3		NCE: CVE		ρΙβ	1	L. //	12	A 1111	I CDII
Denial of	16-12-2016	7.2		ons of NV				tp://nvid			'I-GPU
Service;				s GPU Dis				ısthelp.co		D-	4.6.400
Overflow				a vulneral	•	ıe		pp/answ		0301	16/89
				ode layer			-	detail/a_	id		
			•	km.sys) h			/4	257			
				scape wh		ıe					
				rom a use							
			driver is	used witl	hout						
			validatio	n as the s	ize input	to					
			memcpy	(), causin	g a buffer	•					
			overflow	, leading	to denial	of					
			service o	r potenti	al escalat	ion					
			of privile	eges.							
				NCE: CVE	-2016-8	817					
Denial of	16-12-2016	7.2		ons of NV			htt	tp://nvid	lia	A-NV	'I-GPU
Service				s GPU Dis		er		isthelp.co		D-	
				a vulneral				pp/answ			16/90
				ode layer	•	10		detail/a_		0001	10/00
				km.sys) h		r	-	257	ıu		
				scape wh			/ 4	_0/			
			0	rom a use		10					
			•	used witl							
				on as the i		H					
			-	ading to d							
				r potenti	ai escalat	ion					
			of privile	0	10046.00	04.6					
			KEFERE	NCE: CVE	-2016-8	816					
CV	-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8		8-9	9-10
Scoring	-1 1-2	2-3	3-4	4-3	3 <b>-0</b>	0-	′	7-0		J-9	<del>5-</del> 10
Scale											

CV Scoring Scale	-1 1-2	2-3	3-4 4-5 5-6 6	-7 7-8	8-9 9-10
Execute Code; Overflow	22-12-2016	6.8	openjpeg: A heap-based buffer overflow flaw was found in the patch for CVE-2013-6045. A crafted j2k image could cause the application to crash, or potentially execute arbitrary code.	NA	A-OPE- OPENJ- 030116/94
<i>Openjpeg</i> OpenJPEG is an	open-source [P]	EG 2000	codec written in C language.		
Openjpeg					
			escalation of privileges. <b>REFERENCE: CVE-2016-8813</b>		
			denial of service or potential		
			checking for NULL, leading to		
			DxgDdiEscape where multiple pointers are used without		
			(nvlddmkm.sys) handler for	/4257	
			kernel mode layer	s/detail/a_id	
Service			Windows GPU Display Driver contain a vulnerability in the	.custhelp.com /app/answer	D- 030116/93
Denial of	16-12-2016	7.2	All versions of NVIDIA	http://nvidia	A-NVI-GPU
			<b>REFERENCE: CVE-2016-8814</b>		
			escalation of privileges.		
			checking for NULL, leading to denial of service or potential		
			pointers are used without		
			DxgDdiEscape where multiple		
			(nvlddmkm.sys) handler for	/4257	
			kernel mode layer	s/detail/a_id	030110/92
Service			Windows GPU Display Driver contain a vulnerability in the	.custhelp.com /app/answer	D- 030116/92
Denial of	16-12-2016	7.2	All versions of NVIDIA	http://nvidia	A-NVI-GPU
			<b>REFERENCE: CVE-2016-8815</b>		
			of privileges.		
			array, leading to denial of service or potential escalation		
			validation as the index to an		
			driver is used without		
			passed from a user to the		
			DxgDdiEscape where a value	, 1237	
			kernel mode layer (nvlddmkm.sys) handler for	s/detail/a_id /4257	
			contain a vulnerability in the	/app/answer	030116/91
Service			Windows GPU Display Driver	.custhelp.com	D-
Denial of	16-12-2016	7.2	All versions of NVIDIA	http://nvidia	A-NVI-GPU

				REFERE	NCE: CVE	-2016-9	675				
<b>Pivotal Softv</b>	vare										
Cloud Found Cloud Found and applicati	ry is an	open platf				_	of cloud	ds, develop	er fr	amew	orks,
NA	16-	12-2016	5.8	An open redirect vulnerability has been detected with some Pivotal Cloud Foundry Elastic Runtime components. Users of affected versions should apply the following mitigation: Upgrade PCF Elastic Runtime 1.8.x versions to 1.8.12 or later. Upgrade PCF Ops Manager 1.7.x versions to 1.7.18 or later and 1.8.x versions to 1.8.10 or later. REFERENCE: CVE-2016-6657						A-PIV CLOU 0301	
	ry is an	open platf	orm as a	service, p	roviding a	a choice o		•			
Gain Privileges		12-2016	2.6	Cloud Foundry before 248; UAA 2.x before 2.7.4.12, 3.x before 3.6.5, and 3.7.x through 3.9.x before 3.9.3; and UAA bosh release (aka uaa-release) before 13.9 for UAA 3.6.5 and before 24 for UAA 3.9.3 allow attackers to gain privileges by accessing UAA logs and subsequently running a specially crafted application that interacts with a configured SAML provider.			ugh use) nd ow by	https://ww .cloudfound y.org/Reference: CVE- 2016-6659	vw dr re	A-PIV	7-
Greenplum Greenplum D	atahas	e is an adv	anced fu	lly feature	ed onen so	nurce dat	a war	ehouse			
NA NA		12-2016	6.5	Ily featured, open source data wa An issue was discovered in Pivotal Greenplum before 4.3.10.0. Creation of external tables using GPHDFS protocol has a vulnerability whereby arbitrary commands can be injected into the system. In order to exploit this			al col	https://piv al.io/secur /Reference CVE-2016- 6656	ity	A-PIV GREE 0301	
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	8-9	9-10

Rabbitmq			have sup access to been gra permissi a GPHDF	oility the uperuser 'gpothe system of the sy	padmin' em or hav DFS prot der to cre l table.	re ocol rate					
RabbitMQ is op Protocol (AMQI		age brok	er softwa	re that im	plements	the A	dvance	ed Mes	ssage	Que	uing
NA	29-12-2016	7.5	Pivotal F 3.5.8 and RabbitM 1.5.20, 1 1.7.x bef Telemett connecti a userna succeeds usernam passwor connecti Connecti a client-j are not a	was discondi	3.x before 3.6.6 1.5.x before 3.6.6 1.5.x before 1.6.12, a MQTT (Mort) attication word pair sting ded but the from the fits.	e and ore and IQ with he he	https:, al.io/s /Refer CVE-2 9877	ecurit ence:	y R	-PIV ABB 3011	
Python  Python		. fon anoa	uting and .	undating N	Mi ava a a ft	Mond	l ( da av	) filos			
python-docx is NA	21-12-2016	6.8	python-c allows co attacker External via a cra	lpdating I docx befor ontext-dep s to condu Entity (X) fted docur NCE: CVE	re 0.8.6 pendent act XML XE) attac ment.	ks	NA	j iiles	A P	-PYT YTH 3011	
Qemu											
<b>Qemu</b> QEMU is a gene	ric and open so	urce mad	chine emu	lator and	virtualize	er.					
Bypass; Gain Information	29-12-2016	2.1	QEMU (a built wit emulatio vulnerab derefere	ika Quick h the USB on suppor ole to a nu nce flaw. I nen an app	Emulator EHCI t is ll pointer It could	1)	https:/ lla.red m/sho cgi?id= 43	hat.co w_bu	g. Q	-QEN EMU 3011	
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9		9-10

			attempts to write to EHCI capabilities registers. A privileged user inside quest could use this flaw to crash the QEMU process instance resulting in DoS.  REFERENCE: CVE-2016-2198		
Bypass	29-12-2016	2.1	QEMU (aka Quick Emulator) built with an IDE AHCI emulation support is vulnerable to a null pointer dereference flaw. It occurs while unmapping the Frame Information Structure (FIS) and Command List Block (CLB) entries. A privileged user inside guest could use this flaw to crash the QEMU process instance resulting in DoS.  REFERENCE: CVE-2016-2197	https://bugzi lla.redhat.co m/show_bug. cgi?id=13020 57	A-QEM- QEMU- 030116/101
Cross Site Scripting	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the e1000 NIC emulation support is vulnerable to an infinite loop issue. It could occur while processing data via transmit or receive descriptors, provided the initial receive/transmit descriptor head (TDH/RDH) is set outside the allocated descriptor buffer. A privileged user inside guest could use this flaw to crash the QEMU instance resulting in DoS.  REFERENCE: CVE-2016-1981	https://bugzi lla.redhat.co m/show_bug. cgi?id=12985 70	A-QEM- QEMU- 030116/102
Bypass	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the TPR optimization for 32-bit Windows guests support is vulnerable to a null pointer dereference flaw. It occurs while doing I/O port write operations via hmp interface. In that, 'current_cpu' remains null, which leads to the null	https://bugzi lla.redhat.co m/show_bug. cgi?id=12839 34	A-QEM- QEMU- 030116/103
CV Scoring Scale	0-1 1-2	2-3	3-4 4-5 5-6 6-	7-8	8-9 9-10

CV									
NA	29-12-201	16 2.1	built wit Ethernet	ka Quick h the Cold Controlle is vulnera	Fire Fast er emulat	or lla	tps://bug a.redhat.c /show_bu gi?id=140	o Ql ug. 03	QEM- EMU- 30116/107
Information			Device e vulnerat leakage i while pr 'VIRTIO_ T_INFO' user/pro flaw to le host men	GPU_CMD command ocess coul- eak conter nory byte NCE: CVE	upport is aformation ould occur of GET_CA and guest duse this of the s.	on r .PSE s		03	EMU- 30116/106
Gain	29-12-201 29-12-201		built with Device evulnerable leakage while up in updat guest usthis flaw bytes, rehost.  REFERE  QEMU (2000)	tka Quick the the Virtimulator so le to a me assue. It conditions the ecursor of the control of	o GPU upport is mory ould occur c cursor o data_virg s could u ost memo DoS for a -2016-98	r lata l. A se ory		QI 03	QEM- QEM-
Denial of Service	29-12-201	16 2.1	process crash the resulting <b>REFERE</b> The cpu_phy om_interin QEMU does not regions, privilege a denial crash) vi <b>CVE-20</b> 1 https://	dereference could use e QEMU in gin DoS is NCE: CVE e could use e	this flaw astance, sue2016-19 aory_writ on in execk Emulaiskip MM bows local sers to ca (guest fied vectors)	922 N. e_r ec.c tor) IO use ors.	A	Ql	-QEM- EMU- 30116/104

				descript set outsi	al receive/ or head (T de the allo or buffer.	DH/RDH cated	I) is					
NA	29-1	12-2016	2.1	built wit emulation vulnerable issue. It procession receive of	nka Quick h the e100 on support ole to an ir could occu ng data vi descriptor	00 NIC is finite loo r while a transm s, provid	op it or ed	lla. m/	ps://bu redhat.c show_b ?id=129	o ug.	A-QE QEM 0301	
				built with emulation vulnerable derefered while und Information and Comentries. In inside guito crash instance	th an IDE Appropriate to a number of the contract of the contract of the contract of the QEMU resulting NCE: CVE	HCI is I pointer t occurs the Fram ure (FIS) Block (O ed user use this process in DoS.	e ) CLB)	lla. m/	redhat.c /show_bi ?id=130	o ug.	QEM	
NA		12-2016	2.1	occur which in 'mcf_f privilege guest co crash the host lead REFERE QEMU (abuilt with emulation vulnerable derefered occur what tempts capability privilege could us QEMU presulting REFERE	oop issue. nile receive ec_receive ed user/pr uld use the e QEMU pr ding to Do NCE: CVE aka Quick the USB on support ole to a nu- nce flaw. I nen an app s to write to cies registe ed user ins e this flaw rocess ins g in DoS. NCE: CVE	ing packer'. A ocess insign sissue to compare the contract of	t the 198	lla. m/ cgi 43	ps://bu; redhat.c /show_bi ?id=130 ps://bu;	o ug. 16	A-QE QEM 0301	U- 16/108

			user inside guest could use this flaw to crash the QEMU instance resulting in DoS. <b>REFERENCE: CVE-2016-1981</b>		
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the TPR optimization for 32-bit Windows guests support is vulnerable to a null pointer dereference flaw. It occurs while doing I/O port write operations via hmp interface. In that, 'current_cpu' remains null, which leads to the null pointer dereference. A user or process could use this flaw to crash the QEMU instance, resulting in DoS issue.  REFERENCE: CVE-2016-1922	https://bugzi lla.redhat.co m/show_bug. cgi?id=12839 34	A-QEM- QEMU- 030116/111
Denial of Service	29-12-2016	2.1	The cpu_physical_memory_write_r om_internal function in exec.c in QEMU (aka Quick Emulator) does not properly skip MMIO regions, which allows local privileged guest users to cause a denial of service (guest crash) via unspecified vectors. CVE-2015-8818	https://bugzi lla.redhat.co m/show_bug. cgi?id=13007 71	A-QEM- QEMU- 030116/112
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with a VMWARE VMXNET3 paravirtual NIC emulator support is vulnerable to crash issue. It could occur while reading Interrupt Mask Registers (IMR). A privileged (CAP_SYS_RAWIO) guest user could use this flaw to crash the QEMU process instance resulting in DoS.  CVE-2015-8745	https://bugzi lla.redhat.co m/show_bug. cgi?id=12708 76	A-QEM- QEMU- 030116/113
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with a VMWARE VMXNET3 paravirtual NIC emulator support is vulnerable	http://git.qe mu.org/?p=q emu.git;a=co mmitdiff;h=a	A-QEM- QEMU- 030116/114
CV Scoring Scale	0-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10

				to crash issue. It occurs when a guest sends a Layer-2 packet smaller than 22 bytes. A privileged (CAP_SYS_RAWIO) guest user could use this flaw to crash the QEMU process instance resulting in DoS. CVE-2015-8744					78b36fca f469563l			
NA		2-2016	3.6	QEMU (aka Quick Emulator) built with the NE2000 device emulation support is vulnerable to an OOB r/w access issue. It could occur while performing 'ioport' r/w operations. A privileged (CAP_SYS_RAWIO) user/process could use this flaw to leak or corrupt QEMU memory bytes.  CVE-2015-8743			lla. m/ cgi 29	ps://bug redhat.c show_bu ?id=126	o 1g. 49		U- 16/115	
NA	29-1	2-2016	2.1	built with emulation vulneral error. It processing descript routine, have money (ROCKE fragment inside ground to cause the host process DoS issue the modes of the control	aka Quick in the Rock on support ole to an or happens with the Rock or in 'tx_o' if a descripe than all R_TX_FRA ts. A privilatest could memory lor crash tinstance re.  15-8701	ter switch is ff-by-one while it (tx) consume ptor was owed GS_MAX= eged use this deakage of the QEMU	to =16) er flaw	lla. m/	ps://bug redhat.c show_bu ?id=128	o ıg.	A-QE QEM 0301	
Rapid7												
Nexpose Rapid7 Nexpose is a vulnerability scanner which aims to support the entire vulnerability manageme lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting armitigation.  Cross Site 20-12-2016 3.5 In the Create Tags page of the https://help. A-RAP-								ing and				
Scripting				Rapid7 Nexpose version 6.4.12 user interface, any			4.12	1 /			NEXE	
CV				user inte	errace, any			nex	xpose/er	1-	0301	16/117
CV Scoring Scale	1	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8	3-9	9-10

			authenticated user who has	us/release-	
			the capability to create tags can inject cross-site scripting	notes/#6.4.1	
			(XSS) elements in the tag name field. Once this tag is viewed in		
			the Tag Detail page of the		
			Rapid7 Nexpose 6.4.12 UI by		
			another authenticated user,		
			the script is run in that user's browser context.		
			REFERENCE: CVE-2016-9757		
Roundcube					
Webmail					
		_	source webmail software for the i		
Cross Site	20-12-2016	4.3	Cross-site scripting (XSS)	https://githu	A-ROU-
Scripting			vulnerability in Roundcube Webmail before 1.2.0 allows	b.com/round cube/roundc	WEBMA- 030116/118
			remote attackers to inject	ubemail/issu	030110/110
			arbitrary web script or HTML	es/5240	
			via the href attribute in an area	05,5210	
			tag in an e-mail message.		
			<b>REFERENCE: CVE-2016-4552</b>		
Cross Site	20-12-2016	4.3	Cross-site scripting (XSS)	NA	A-ROU-
Scripting			vulnerability in Roundcube		WEBMA-
			Webmail before 1.2.0 allows		030116/119
			remote attackers to inject arbitrary web script or HTML		
			via the href attribute in an area		
			tag in an e-mail message.		
			<b>REFERENCE: CVE-2016-4552</b>		
S9Y	•				
<b>Serendipity</b> Serendipity is a	a PHP-powered v	veblog e	ngine which gives the user an eas	y way to mainta	in a blog.
Cross Site	25-12-2016	3.5	Multiple cross-site scripting	NA	A-S9Y-
Scripting			(XSS) vulnerabilities in		SEREN-
			Serendipity before 2.0.5 allow		030116/120
			remote authenticated users to		
			inject arbitrary web script or HTML via a category or		
			directory name.		
			REFERENCE: CVE-2016-9681		
Siemens					
Desigo Web M	odule Pxa30-w0	Firmw	are;Desigo Web Module Pxa30-v	v1 Firmware;De	esigo Web
			Veb Module Pxa40-w0 Firmware		

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

w1 Firmware;l	Desigo Web Mod	dule Pxa	40-w2 Firmware		
NA Simatic Pcs 7;S		5	Siemens Desigo PX Web modules PXA40-W0, PXA40-W1, PXA40-W2 for Desigo PX automation controllers PXC00-E.D, PXC50-E.D, PXC100-E.D, PXC200-E.D (All firmware versions < V6.00.046) and Desigo PX Web modules PXA30-W0, PXA30-W1, PXA30-W2 for Desigo PX automation controllers PXC00-U, PXC64-U, PXC128-U (All firmware versions < V6.00.046) use a pseudo random number generator with insufficient entropy to generate certificates for HTTPS, potentially allowing remote attackers to reconstruct the corresponding private key.  REFERENCE: CVE-2016-9154	NA	A-SIE- DESIG- 030116/121
process, from g	oods receipt to	goods is:	A vulnerability in SIEMENS SIMATIC WinCC (All versions < SIMATIC WinCC (All versions < SIMATIC WinCC V7.2) and SIEMENS SIMATIC PCS 7 (All versions < SIMATIC PCS 7 V8.0 SP1) could allow a remote attacker to crash an ActiveX component or leak parts of the application memory if a user is tricked into clicking on a malicious link under certain conditions.  REFERENCE: CVE-2016-9160	rocess plants; SI	MATIC WinCo
CV Scoring Scale	-1 1-2	2-3	3-4 4-5 5-6 6-	7-8	8-9 9-10

Tarantool												
Msgpuck												
msgpuck is a s	imple	and efficie	nt MsgPa	ack binary	y serializat	tion libra	ry in a	a se	lf-contai	ned	heade	er file.
Denial of Service	23-	12-2016	5	An exploitable incorrect return value vulnerability exists in the mp_check function of Tarantool's Msgpuck library 1.0.3. A specially crafted packet can cause the mp_check function to incorrectly return success when trying to check if decoding a map16 packet will read outside the bounds of a buffer, resulting in a denial of service vulnerability.  REFERENCE: CVE-2016-9036					<b>A</b>		A-TA MSG 0301	
Tarantool		N	COL 1.	1			1.7		1: .:			
Tarantool is an										n se		<u> </u>
Denial of Service	23-	12-2016	7.8	array accexists in xrow_he of Taran A specia cause the element a global determinal specified lead to a within the server. A exploits cause a covulneral	oitable out cess vulne the ader_deco tool 1.7.2. Illy crafted e function outside tharray that ne the type I key's val n out of bene context an attackethis vulnedenial of solity on the NCE: CVE	erability ode functi 0-g8e927 packet c to access ne bounds is used t e of the ue. This c ounds rea f of the r who rability c ervice ne server.	ion 715. an s an s of o can ad	NA	1		A-TA TARA 0301	
Vmware												
Fusion VMware Fusion without rebood Bypass; Gain	ting.	he easiest, 12-2016	fastest a	VMware	Fusion 8.	x before 8	8.5	htt	p://www	w.	A-VM	IW-
Information				Protection	when Sys on (SIP) is ocal users	enabled,	,	/security/ad 03		FUSI 0301	0- 16/125	
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8		8-9	9-10

			kernel memory addresses and bypass the kASLR protection mechanism via unspecified vectors.  REFERENCE: CVE-2016-5329	A-2016- 0017.html						
Fusion: Fusion	Pro: Workstati	on Play								
Fusion; Fusion Pro; Workstation Player; Workstation Pro VMware Fusion Pro and VMware Fusion let anyone run Windows and hundreds of other operating										
systems on a Mac, without rebooting; VMware Workstation Pro and VMware Workstation Player are										
the industry standard for running multiple operating systems as virtual machines on a single PC.										
Denial of	29-12-2016	7.2	The drag-and-drop (aka DnD)	http://www.	A-VMW-					
Service,	27-12-2010	7.2	function in VMware	vmware.com	FUSIO-					
Execute Code;			Workstation Pro 12.x before							
•				/security/ad	030116/126					
Overflow			12.5.2 and VMware	visories/VMS						
			Workstation Player 12.x before	A-2016-						
			12.5.2 and VMware Fusion and	0019.html						
			Fusion Pro 8.x before 8.5.2							
			allows guest OS users to							
			execute arbitrary code on the							
			host OS or cause a denial of							
			service (out-of-bounds							
			memory access on the host OS)							
			via unspecified vectors.							
			<b>REFERENCE: CVE-2016-7461</b>							
Horizon View	n View is the wi	rtual dec	sktop host platform for vSphere.							
Directory	29-12-2016	5	Directory traversal	http://www.	A-VMW-					
Traversal;	27 12 2010	3	vulnerability in the Connection	vmware.com	HORIZ-					
Gain			Server in VMware Horizon	/security/ad	030116/127					
Information			View 5.x before 5.3.7, 6.x	visories/VMS	030110/127					
IIIIOIIIIatioii			before 6.2.3, and 7.x before	A-2016-						
			•	0015.html						
			7.0.1 allows remote attackers	0015.111111						
			to obtain sensitive information							
			via unspecified vectors.							
13	I		REFERENCE: CVE-2016-7087							
Identity Mange				# 1 :1 Cl 1	E D 1					
	•		dentity Management for the M		era; vRealize					
			automates the delivery of IT serv		A 1784147					
NA	29-12-2016	5	VMware Identity Manager 2.x	http://www.	A-VMW-					
			before 2.7.1 and vRealize	vmware.com	IDENT-					
			Automation 7.x before 7.2.0	/security/ad	030116/128					
			allow remote attackers to read	visories/VMS						
			/SAAS/WEB-INF and	A-2016-						
			/SAAS/META-INF files via	0021.html						
			unspecified vectors.							
			REFERENCE: CVE-2016-5334							
CV 0.	-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10					
Scoring Scale										
Jeane										

<b>Tools</b> VMware Tools	is an ontional, fr	ree set o	f drivers and utilities that enhan	ces both the ner	formance of a
			m and interaction between the gu		
Denial of Service; Gain	29-12-2016	4.6	The graphic acceleration functions in VMware Tools 9.x	http://www. vmware.com	A-VMW- TOOLS-
Privileges			and 10.x before 10.0.9 on OS X	/security/ad	030116/129
			allow local users to gain	visories/VMS	,
			privileges or cause a denial of	A-2016-	
			service (NULL pointer	0014.html	
			dereference) via unspecified vectors, a different		
			vulnerability than CVE-2016-		
			7079.		
			REFERENCE: CVE-2016-7080		
Denial of	29-12-2016	4.6	The graphic acceleration	http://www.	A-VMW-
Service; Gain			functions in VMware Tools 9.x	vmware.com	TOOLS-
Privileges			and 10.x before 10.0.9 on OS X allow local users to gain	/security/ad visories/VMS	030116/130
			privileges or cause a denial of	A-2016-	
			service (NULL pointer	0014.html	
			dereference) via unspecified		
			vectors, a different		
			vulnerability than CVE-2016-		
			7080. <b>REFERENCE: CVE-2016-7079</b>		
Bypass	29-12-2016	2.1	VMware Tools 9.x and 10.x	http://www.	A-VMW-
Буразз	27 12 2010	2.1	before 10.1.0 on OS X, when	vmware.com	TOOLS-
			System Integrity Protection	/security/ad	030116/131
			(SIP) is enabled, allows local	visories/VMS	
			users to determine kernel	A-2016-	
			memory addresses and bypass	0017.html	
			the kASLR protection mechanism via unspecified		
			vectors.		
			REFERENCE: CVE-2016-5328		
Vcenter Server					
			zed management application th	at lets you m	anage virtual
NA	ESXi hosts centra 29-12-2016	ally.	VMware vCenter Server 5.5	http://www.	A-VMW-
INA	27-12-2010	4	before U3e and 6.0 before U2a	http://www. vmware.com	VCENT-
			allows remote authenticated	/security/ad	030116/132
			users to read arbitrary files via	visories/VMS	, ,
			a (1) Log Browser, (2)	A-2016-	
			Distributed Switch setup, or	0022.html	
			(3) Content Library XML		
CV Sacring 0	-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8 <b>-</b> 9 <b>9-10</b>
Scoring Scale					

			document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.  REFERENCE: CVE-2016-745						
Vrealize Auto VMware vReal unified cloud i	lize Automation,	formerl	y called vCloud Automation C	lenter,	is a softv	ware	prod	uct for	
Denial of Service	29-12-2016	6.4	The Single Sign-On feature in VMware vCenter Server 5.5 before U3e and 6.0 before U2 and vRealize Automation 6.x before 6.2.5 allows remote attackers to read arbitrary fill or cause a denial of service vian XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. <b>REFERENCE: CVE-2016-746</b>	les of	ttp://www mware.con security/a isories/VM -2016- 022.html	m ld	A-VM VREA 0301		
responsible for	cations is availab or managing vSp	here an	ree editions (Standard, Adva d virtual infrastructure, hete cture at the OS and application	erogen					
NA	29-12-2016	7.5	The Suite REST API in VMwar vRealize Operations (aka vROps) 6.x before 6.4.0 allow remote authenticated users twrite arbitrary content to file or rename files via a crafted DiskFileItem in a relay-reque payload that is mishandled during deserialization.  REFERENCE: CVE-2016-746	re he vi	ttp://www mware.con security/a isories/VN -2016- 020.html	m ld	A-VM VREA 0301		
Gain Privileges	29-12-2016	8	VMware vRealize Operations (aka vROps) 6.x before 6.4.0 allows remote authenticated users to gain privileges, or ha and remove virtual machines via unspecified vectors.  REFERENCE: CVE-2016-745	m	A-VM VREA 0301				
Vsphere Client  VMware vSphere client is a Windows application for administering VMware vCenter Server and									
CV Scoring Scale	coring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10								

VMware ESX/E	SXi virtualizatio	n platfor	ms.								
NA	29-12-2016	5	VMware vSphere Client 5.5 before U3e and 6.0 before U2a allows remote vCenter Server and ESXi instances to read arbitrary files via an XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. REFERENCE: CVE-2016-7458	http://www. vmware.com /security/ad visories/VMS A-2016- 0022.html	A-VMW- VSPHE- 030116/136						
Vsphere Data Protection VDP is a robust, simple-to-deploy, disk-based backup and recovery solution.											
NA	29-12-2016	10	VMware vSphere Data Protection (VDP) 5.5.x though 6.1.x has an SSH private key with a publicly known password, which makes it easier for remote attackers to obtain login access via an SSH session.  REFERENCE: CVE-2016-7456	http://www. vmware.com /security/ad visories/VMS A-2016- 0024.html	A-VMW- VSPHE- 030116/137						
Workstation Player; Workstation Pro											
VMware Works	station Pro and	VMwar	e Workstation Player are the in	ndustry standar	d for running						
Gain Privileges	29-12-2016	7.2	The installer in VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows allows local users to gain privileges via a Trojan horse setup64.exe file in the installation directory.  REFERENCE: CVE-2016-7086	http://www. vmware.com /security/ad visories/VMS A-2016- 0014.html	A-VMW- WORKS- 030116/138						
Gain Privileges	29-12-2016	7.2	Untrusted search path vulnerability in the installer in VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows allows local users to gain privileges via a Trojan horse DLL in an unspecified directory.	http://www. vmware.com /security/ad visories/VMS A-2016- 0014.html	A-VMW- WORKS- 030116/139						
CV Scoring Scale	-1 1-2	2-3	3-4 4-5 5-6 6-	7-8	8-9 9-10						

			REFERENCE: CVE-20	16-7085		
Denial of Service; Execute Code; Overflow; Memory Corruption	29-12-2016	6.9	pview.dll in VMware Vorkstation Pro 12.x. 2.5.0 and VMware Vorkstation Player 1 2.5.0 on Windows, vortado ThinPrint virtining is enabled, a guest OS users to exembitrary code on the or cause a denial of so host OS memory cortia a JPEG 2000 imag REFERENCE: CVE-20	2.x before when tual llows cute host OS ervice ruption) e.	http://www.vmware.com/security/advisories/VMSA-2016-0014.html	WORKS- 030116/140
Denial of Service; Execute Code; Overflow; Memory Corruption	29-12-2016	5.9	Mware Workstation before 12.5.0 and VM Vorkstation Player 1.2.5.0 on Windows, vortado ThinPrint virorinting is enabled, and S users to execute a code on the host OS of denial of service (host nemory corruption) TrueType fonts embed MFSPOOL.	ware 2.x before when tual llow guest rbitrary or cause a t OS via edded in	http://www.vmware.com /security/ad visories/VMS A-2016- 0014.html	WORKS- 030116/141
Denial of Service; Execute Code; Overflow; Memory Corruption	29-12-2016	5.9	Mware Workstation before 12.5.0 and VM Vorkstation Player 1.2.5.0 on Windows, vortado ThinPrint virorinting is enabled, and S users to execute a ode on the host OS of lenial of service (host nemory corruption) EMF file.  REFERENCE: CVE-20	ware 2.x before when tual llow guest rbitrary or cause a t OS via an	http://www.vmware.com /security/ad visories/VM! A-2016- 0014.html	WORKS- 030116/142
Execute Code; Overflow	29-12-2016	6.9	Multiple heap-based verflows in VMware Vorkstation Pro 12.x 2.5.0 and VMware Vorkstation Player 1 2.5.0 on Windows, v	before  2.x before  vhen	http://www vmware.com /security/ad visories/VMS A-2016- 0014.html	WORKS- 030116/143
Scoring Scale	-1 1-2	2-3	3-4 4-5	5-6 6-7	7 7-8	8-9 9-10

			Cortado ThinPrint virtual		
			printing is enabled, allow guest		
			OS users to execute arbitrary		
			code on the host OS via		
			unspecified vectors.		
			REFERENCE: CVE-2016-7081		
Xmltwig					
Xml-twig For I					
		_	cess efficiently XML documents	1	
NA	22-12-2016	6.4	perl-XML-Twig: The option to	NA	A-XML-XML-
			`expand_external_ents`,		T-
			documented as controlling		030116/144
			external entity expansion in		
			XML::Twig does not work.		
			External entities are always		
			expanded, regardless of the		
			option's setting.		
	_		REFERENCE: CVE-2016-9180		
	Ap	plication	on; Operating System (A/O	<u>S)</u>	
Debian/Xrdp					
Debian Linux/	•	, ,			222
			tribution of Free Software/xrdp		
NA	16-12-2016	5	An issue was discovered in	https://githu	A-OS-DEB-
			xrdp before 0.9.1. When	b.com/neutri	DEBIA-
			successfully logging in using	nolabs/xrdp/	030116/145
			RDP into an xrdp session, the	pull/497	
			file		
			~/.vnc/sesman_\${username}_		
			passwd is created. Its content		
			is the equivalent of the user's		
			cleartext password, DES		
			encrypted with a known key.		
Dahian Fada	commeicate Cours	/IZDE	REFERENCE: CVE-2013-1430		
*	raproject; Suse,		no /Vva ail		
•	Fedora/Linux E	-	•	one (formorly E	odova Covo) ia
	0 .		stribution of Free Software/ Fed	•	
_			nux kernel, developed by the c		
_		-	E Linux Enterprise Server is a wo		_
_		_	r physical, virtual and cloud-base ct, the integrated personal informa		
NA	23-12-2016	7.5	Through a malicious URL that	NA	A-OS-DEB-
1471	25 12 2010	7.5	contained a quote character it	1471	DEBIA-
			was possible to inject HTML		030116/146
			code in KMail's plaintext		030110/140
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					

				1	,				
			viewer. Due to the parser used						
			on the URL it was not possible						
			to include the equal sign (=) or						
			a space into the injected HTML,						
			which greatly reduces the						
			available HTML functionality.						
			Although it is possible to						
			include an HTML comment						
			indicator to hide content.						
			<b>REFERENCE: CVE-2016-7966</b>						
Fedoraproject	<u> </u>								
	Kscreenlocker;								
			perating system based on the Li						
	community-supported Fedora Project and sponsored by Red Hat/ LEAP is an online community for								
			lity and the home of the LEAP so						
			M (Pluggable Authentication Mo	odules) system	for password				
	nlocking the dis								
Denial of	23-12-2016	4.6	Turning all screens off in	NA	A-OS-FED-				
Service			Plasma-workspace and		FEDOR-				
			kscreenlocker while the lock		030116/147				
			screen is shown can result in						
			the screen being unlocked						
			when turning a screen on						
			again.						
			REFERENCE: CVE-2016-2312						
NA	23-12-2016	4.6	Turning all screens off in	https://www	A-OS-FED-				
			Plasma-workspace and	.kde.org/info	FEDOR-				
			kscreenlocker while the lock	/security/ad	030116/148				
			screen is shown can result in	visory-					
			the screen being unlocked	20160209-					
			when turning a screen on	1.txt					
			again.						
			REFERENCE: CVE-2016-2312						
KDE/Novell;O	pensuse Proje	ct							
Kde-cli-tools/L	• / •								
Kde-cli-tools ar	e tools based o	n KDE F	Frameworks 5 to better interact	with the systen	n/ LEAP is an				
	5	-	working for sustainability and th						
			ux and SuSE Linux Professional,	is a Linux-base	ed project and				
distribution spo	onsored by SUSI	E Linux C	mbH and other companies.						
Execute Code	23-12-2016	4	A maliciously crafted	NA	A-OS-KDE-				
			command line for kdesu can		KDE-C-				
			result in the user only seeing 0301						
			part of the commands that will						
			actually get executed as super						
			user.						
CV	-1 1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10				
Scoring	1-2	2-3	3-1 3-0 0-	7-0	J-10				
Scale									

			REFERE	NCE: CVE	-2016-7	787					
Microsoft/Mic	rosoft										
Microsoft Offic computers/Wir system develop	Windows 7;Windows 7;Windows 7 (codens by Microsof ms; Windows Vi	c is by amed Vi t; Windo	far the enna, for ows Serve	most pov merly Bla er 2008 is	verful se ckcomb) s one of	t of p is a p Micros	erso soft V	nal coi Vindov	mpu ws'	iter op server	erating line of
Gain Information	20-12-2016	4.3	The GDI component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office for Mac 2011, and Office 2016 for Mac allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "GDI Information Disclosure Vulnerability." REFERENCE: CVE-2016-7257							A-OS- OFFI 0301	
		01		g System							
Blackberry		<u> </u>	portion	5 by brom	(00)						
Good Enterpris	<b>se Mobility Serv</b> e Mobility Serve dules on a stand	er (GEM			Good Co	nnect	and	Good I	Mob	ile Me	ssaging
Execute Code	16-12-2016	8.5	vulnerate Good En Server (Goof the Ap shell in Good to 2.2.22 attacker administ GEMS see executed comman REFERE	NCE: CVE	e BlackBe Iobility plementa of comma ions 2.1.5 s remote of local of son the ommands araf	erry ation and 5.3	rt.bl com leDe leNu 0003 angu ne	://supj ackber /kb/ar tail?ar mber= 388148 aage=N	ry. tic tic 0 &l		) - 16/151
Execute Code	16-12-2016	8.5	Remote shell execution vulnerability in the BlackBerry Good Enterprise Mobility Server (GEMS) implementation of the Apache Karaf command shell in GEMS versions 2.1.5.3				rt.bl com leDe leNu	://supj ackber /kb/ar tail?ar mber= 388148	ry. tic tic 0	O-BL. GOOI 0301	
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7		7-8		8-9	9-10

Google  Android  Android is a many primarily for to Gain Information		mobile devic	developed es such as The non listener introduce Android Samsung devices, can persafter the upgrade or 6.0.1 system a existent the notification obtain the notification contain introduce and the notification obtain the notification contain introduce and the notification contain introduce and the notification obtain the notification contain interest and the notification contains and t	d by Google smartphorexistent revulnerabile ted in the instance of the second of the s	ts on the ommands araf  -2016-3:  te, based ones and notification ity was nitial device even droid 5.1 vulnerable non-polity to reom the ord-party so a packatoria party applies of tend to lata.	on the tablets of tablets on the tablets on tablets on tablets on the tablets on tablets on the tablets on tab			nel and d	00-
Thinpro										
Gain Privileges; Bypass	is the out-c		for HP Thin Clients.  HP ThinPro 4.4 through 6.1 mishandles the keyboard layout control panel and virtual keyboard application, which allows local users to bypass intended access restrictions and gain privileges				NA		0-HF THIN 0301	
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9	9-10

	via unspecified vectors.  REFERENCE: CVE-2016-2246  29-12-2016 7.2 HP ThinPro 4.4 through 6.1 NA											
Gain Privileges; Bypass	29-1	12-2016	7.2	HP ThinPro 4.4 through 6.1 mishandles the keyboard layout control panel and virtual keyboard application, which allows local users to bypass intended access restrictions and gain privileges via unspecified vectors.  REFERENCE: CVE-2016-2246					ı		0-HF THIN 0301	
Linux												
Linux Kernel Linux Kernel task for Linux	in a Nu				erview of	kernel co	onfigu	ırat	ion and l	ouil	ding, a	critical
Denial of Service		12-2016	7.2	Race cornetlink_net/netlLinux keallows lood or possilother imapplicat sendms to a free with a nearlier to	ndition in addump fund ink/af_net ink/af_net ocal users f service (obly have upact via a ion that mag system coperation ew dump an anticitic in the intervence in the interven	ction in tlink.c in te 4.6.3 to cause double fr nspecifie crafted akes alls, leadi associat that start pated.	a ee) ed ing eed	lla m,	tps://bug .redhat.c /show_bu i?id=140	o ug.	O-LINU USO1	
Denial of Service	28-3	12-2016	4.6	REFERENCE: CVE-2016-9806 Race condition in the snd_pcm_period_elapsed function in sound/core/pcm_lib.c in the ALSA subsystem in the Linux kernel before 4.7 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted SNDRV_PCM_TRIGGER_START command.  REFERENCE: CVE-2016-9794		https://bugzi lla.redhat.co m/show_bug. cgi?id=14014 94		co LINUX- ug. 030116,				
Denial of Service; Overflow;	28-1	12-2016	7.2	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 http://git.ke				it/l LINUX-		X-		
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8		8-9	9-10

Memory Corruption			sk_sndbi which al cause a c (memor system c unspecif leveragi CAP_NE' a crafted call with SO_SNDI	T_ADMIN of setsockorus the (1) BUFFORCI	rcvbuf, users to ervice on and ossibly h impact by capability pt system E or (2)	linu mit b0k ceb	torvald/torvald/torvald/torvald/to.	om 18 e3 df			
Denial of Service, Gain Privileges	28-12-2016	6.9	REFERE KVM in t 4.8.12, w enabled, restrict t allows g host OS denial of bounds a OS crash interrup arch/x86 arch/x86	BUFFORCH NCE: CVE the Linux land A when I/O A does not the VCPU in uest OS us privileges f service (of array acce a) via a cra trequest, 6/kvm/ios 6/kvm/ios 6/kvm/ios	-2016-9' kernel be APIC is properly ndex, wheers to ga or cause out-of- ss and ho fted related to apic.c and	fore  iich in a ost o	nellinu git/ linu mit db2 1c4	p://git.k .org/cgi x/kerne /torvald ix.git/co /?id=81 259fb6d ecfeea3 5a73c07	t/l el/ s/ om .c 8c 8		X- 16/159
Gain Information	28-12-2016	2.1	the Linu does not Code Seg error cas users to informat memory applicat		efore 4.8 initialize ) in certa allows lo isitive kernel sta	in ocal ack	b.co ds/ mm 539 bf8	os://gitl om/torv linux/co nit/2117 98c8155 03f5fd1 eb78216	ral o 7d 54f dc	O-LINU LINU 0301	
Denial of Service; Overflow	28-12-2016	4.6	REFERENCE: CVE-2016-9756  The netfilter subsystem in the Linux kernel before 4.9 mishandles IPv6 reassembly, which allows local users to cause a denial of service (integer overflow, out-of-bounds write, and GPF) or possibly have unspecified				b.co ds/ mm a06 ed7	ps://gitl om/torv linux/co nit/9b57 530c9fd3 7a20fc0f 582cc07	ral o 7d 36 59	O-LIN LINU 0301	
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8	8-9	9-10

			other impact via a crafted application that makes socket, connect, and writev system calls, related to net/ipv6/netfilter/nf_conntrac k_reasm.c and net/ipv6/netfilter/nf_defrag_i pv6_hooks.c.  REFERENCE: CVE-2016-9755		
Denial of Service	28-12-2016	4.9	Multiple memory leaks in error paths in fs/xfs/xfs_attr_list.c in the Linux kernel before 4.5.1 allow local users to cause a denial of service (memory consumption) via crafted XFS filesystem operations.  REFERENCE: CVE-2016-9685	http://git.ker nel.org/cgit/l inux/kernel/ git/torvalds/ linux.git/com mit/?id=2e8 3b79b2d6c7 8bf1b4aa227 938a214dcb ddc83f	O-LIN- LINUX- 030116/162
Denial of Service	28-12-2016	2.1	arch/x86/kvm/vmx.c in the Linux kernel through 4.9 mismanages the #BP and #OF exceptions, which allows guest OS users to cause a denial of service (guest OS crash) by declining to handle an exception thrown by an L2 guest.  REFERENCE: CVE-2016-9588	http://git.ker nel.org/cgit/l inux/kernel/ git/torvalds/ linux.git/com mit/?id=ef85 b67385436d dc1998f45f1 d6a210f935b 3388	O-LIN- LINUX- 030116/163
Denial of Service	28-12-2016	7.2	The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 4.8.14 does not properly restrict the type of iterator, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device.  REFERENCE: CVE-2016-9576	http://git.ker nel.org/cgit/l inux/kernel/ git/torvalds/ linux.git/com mit/?id=a0ac 402cfcdc904f 9772e1762b 3fda112dcc5 6a0	O-LIN- LINUX- 030116/164
Gain Privileges	28-12-2016	6.9	kernel/events/core.c in the performance subsystem in the Linux kernel before 4.0 mismanages locks during	http://git.ker nel.org/cgit/l inux/kernel/ git/torvalds/	O-LIN- LINUX- 030116/165
CV Scoring Scale	1-2	2-3	3-4 4-5 5-6 6-	7 7-8	8-9 9-10

			contain	nigrations	which		linn	v git /gg	m		
				nigrations ocal users				x.git/co /?id=f6:			
							,	a5812a			
				es via a cra				6c9623			
				ion, aka Ai				7e1ff9c			
				bug 3109 <b>NCE: CVE</b>		707		/e11190	CD		
Cair	20.12.2016	( ()					2b	. / / - 1 1		0.11	A.T.
Gain	28-12-2016	6.9	,	events/co				://git.k		O-LII	
Privileges			•	ance subs		tne		org/cgi	,	LINU	
				rnel befor				k/kerne	•	0301	16/166
				ages locks	_			torvald			
				nigrations				x.git/co			
				cal users	_			/?id=f6:			
				es via a cra				a5812a			
				ion, aka Ai				6c9623			
				bug 3095		<b>-</b> 06		7e1ff9c	cb		
D . 1 . 6	00.40.0046	. –		NCE: CVE			2b			0.7.7	
Denial of	28-12-2016	4.7		space.c in		X	-	s://gitl		O-LII	
Service				efore 4.9 o				m/torv		LINU	
				now many		-	-	linux/co		0301	16/167
				mount n	_			it/d292			
				lows local				2a85c7			
				denial of s		_		536108			
			`	y consum <sub>]</sub>	•			963f02	71		
				k) via MS_			449	8			
			-	alls, as de		ted					
			-	that trigg	_						
			•	tial growt							
				of mounts							
				NCE: CVE							
Denial of	28-12-2016	7.2		_setsocko	_		_	://git.k		O-LII	
Service;			,	ore/sock.o				org/cgi	•	LINU	
Overflow;				efore 3.5 ı				k/kerne	•	0301	16/168
Memory				values of	<del>-</del>		· ,	torvald	•		
Corruption				cvbuf, wh				x.git/co			
				rs to caus				/?id=82			
				memory o				30125a			
			and syst	em crash)	or possi	bly	d39	d7c837	8'		
				specified o	other imp	act	a9ct	fdf5e1b	e2		
			by lever	aging the			002	b			
			CAP_NE	Γ_ADMIN	capability	y for					
			a crafted setsockopt system								
			call with the (1) SO_SNDBUF or								
			(2) SO_R	CVBUF or	otion.						
			CVE-202	12-6704							
CV	1 12	2.2	2.4	4.5	<b>F</b> (		,	7.0		0.0	0.40
Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7		7-8		8-9	9-10

## Microsoft

Scale

Windows 10; Windows 7; Windows 8.1; Windows Rt 8.1; Windows Server 2008; Windows Server 2012; Windows Server 2016; Windows Vista

Microsoft Windows is a meta-family of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems which cater to a certain sector of the computing industry with the OS typically associated with IBM PC compatible architecture.

computing industry with the OS typically associated with IBM PC compatible architecture.												
Gain Information	20-	12-2016	2.1		nmon Log l Iriver in M		em	NA	1		O-MI WINI	_
				` ,	s Vista SP		ws					16/169
					008 SP2 a							,
				Window	s 7 SP1, W	indows 8	8.1,					
				Window	s Server 2	012 Gold	l					
				and R2,	Windows 1	RT 8.1,						
				Window	s 10 Gold,	1511, an	ıd					
					id Window							
					ows local ı							
					ensitive in							
				•	cess mem	•	l					
					pplication							
					vs Commo	_						
				-	Oriver Info							
					re Vulnera		205					
Cain	20	12 2017	7.2		NCE: CVE		295	NI A			O MI	C
Gain	20-	12-2016	7.2		aller in Mi			NA	1		O-MI	
Privileges					s Vista SP2 008 SP2 a						WINI	16/170
					s 7 SP1, W						0301	10/1/0
					s 7 31 1, w							
					Windows 1		•					
					s 10 Gold,		ьd					
					d Window							
					shandles l							
					which allo							
					gain privil							
					pplication	_						
					vs Installe		on					
				of Privile	ege Vulner	ability."						
					NCE: CVE		292					
Execute Code	20-	12-2016	9.3	Uniscribe in Microsoft				NA	1		O-MI	
					s Vista SP	•					WINI	
				Server 2008 SP2 and R2 SP1,							0301	16/171
				Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and								
	<u> </u>			window	s 10 Gold,	1511, an	ıa					
CV Scoring 0	-1	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8	8-9	9-10

Execute Code		-12-2016	9.3	2016 all to execu crafted we will window REFERE Microso Window R2 SP1, Window 2012 Go RT 8.1, Window 2012 REFERE REFERE		te attackery code vika be Remoralinerability -2016-72 ponent in vista Si 008 SP2 7 SP1, dows Ser Window 10 Gold, and Window 10 Gold, and Window 10 Femote te arbitra web site, as Remotalinerability	ers ia a  te ty."  274  P2, and ever as  ary aka e ty."	NA			O-MI WINI 0301	00- 16/172		
Gain Privileges	20-	-12-2016	7.2	REFERENCE: CVE-2016-7272  The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."					NA			WINDO- 030116/173		
Gain Privileges	20-	-12-2016	7.2	REFERENCE: CVE-2016-7260				NA		O-MIC- WINDO- 030116/174				
CV Scoring Scale	-1	1-2	2-3	3-4	4-5	5-6	6-'	7	7-8		8-9	9-10		

			applicat Elevatio Vulneral	orivileges vion, aka "Vin of Privile bility." SNCE: CVE	Vin32k ege							
Gain Information	20-12-2016	2.1	Window Server 2 Window and R2, Window 1607, an 2016 all obtain so via a cra "Window Informa" Vulneral	,	2, Windo nd R2 SP Indows 8 012 Gold RT 8.1, 1511, an vs Server users to formatio cation, ak Driver osure	ws 1, 3.1, 1 1 1 1 1 1	NA			0-MI WINI 0301		
Execute Code	20-12-2016	9.3	The Graphics component in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Windows Graphics Remote Code Execution Vulnerability."  REFERENCE: CVE-2016-7273					NA			O-MIC- WINDO- 030116/176	
Bypass	20-12-2016	4.6	impleme Window 1607 an 2016 all bypass t (VTL) pr via a cra "Secure of Privile	are Kernel entation in a 10 Gold, d Window ows local to the virtual rotection rated applicated Wernel Mcege Vulner	Microso 1511, and as Server users to trust lever nechanistication, akede Eleva rability."	el m ca tion	NA			O-MIC- WINDO- 030116/177		
Gain Information	20-12-2016	2.1	Window 1607 an 2016 mi	nel in Micr rs 10 Gold, d Window shandles p calls, whicl	1511, an s Server page-faul		NA		0-MIC- WINDO- 030116/178			
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8	8-9	9-10	

Scoring Scale	1 1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8	3-9	9-10
Denial of Service	16-12-2016	7.8	A vulnerability in SIEMENS http://www. O-SIE SIMATIC S7-300 PN CPUs (all siemens.com SIMA'								
NA Gain Information	16-12-2016	4.3	A vulnerability in SIEMENS SIMATIC S7-300 PN CPUs (all versions including V3.2.12) and SIMATIC S7-400 PN CPUs (all versions including V7) could allow a remote attacker to obtain credentials from the PLC if protection-level 2 is configured on the affected devices.  REFERENCE: CVE-2016-9159				http://www.siemens.com /cert/pool/c ert/siemens_ security_advi sory_ssa- 731239.pdf		m /c s_ vi	O-SIE- SIMAT- 030116/180	
Siemens Simatic S7-300	Cpu Firmware	e;Simatio	: <b>S7-400</b> (	Spu Firmv	vare						
Redhat  Enterprise Linu Server;Enterpr Red Hat Enterp the commercial Gain Information	<b>ise Linux Work</b> rise Linux (RH	station	sktop;Ent Linux dist sudo: It the defar on Red H and poss impleme value of lead to in A local u to a rest uses rea flaw to r specially elevated by sudo.	erprise Literprise Lit	develope vered that onfigurate orise Linux oreserves which co n disclosi udo acce gram that d use this nt from d files wi s provide	Node d by t tion x the uld ure. ss t t d		Hat and		geted O-RE ENTE	D-
			local users to obtain sensitive information from arbitrary processes via a crafted application, aka "Windows Kernel Memory Address Information Disclosure Vulnerability."								

			and SIMATIC S7-400 PN CPUs (V6 and V7) could allow a remote attacker to cause a Denial of Service condition by sending specially crafted packets to port 80/TCP. <b>REFERENCE: CVE-2016-9158</b>	ert/siemens_ security_advi sory_ssa- 731239.pdf	
Technicolor					
Xfinity Gatewo	ay Router Dpc39	41t Firi	nware		
Cross Site Request Forgery	16-12-2016	7.9	CSRF vulnerability on Technicolor TC dpc3941T (formerly Cisco dpc3941T) devices with firmware dpc3941-P20-18- v303r20421733-160413a- CMCST allows an attacker to change the Wi-Fi password, open the remote management interface, or reset the router. REFERENCE: CVE-2016-7454	NA	O-TEC- XFINI- 030116/182
Vmware					
<b>Esxi</b> VMware ESXi i	s the industry-le	ading, pı	urpose-built bare-metal hyperviso	or.	
Cross Site Scripting	29-12-2016	3.5	Cross-site scripting (XSS) vulnerability in the Host Client in VMware vSphere Hypervisor (aka ESXi) 5.5 and 6.0 allows remote authenticated users to inject arbitrary web script or HTML via a crafted VM. REFERENCE: CVE-2016-7463	http://www. vmware.com /security/ad visories/VMS A-2016- 0023.html	O-VMW- ESXI- 030116/183

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