	National Cri	itical I	nformation Infrastructu <i>CVE Report</i> 01-15 February 2017		entre 1. 04 No. 03
Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
	2000		Application (A)	1	I
Adobe					
<i>Campaign</i> Adobe Campaign goals.	, part of Adob	e Marke	eting Cloud, helps you achiev	e your cross-chan	nel marketing
Cross Site Scripting	15-02-2017	4.3	Adobe Campaign versions 16.4 Build 8724 and earlier have a cross-site scripting (XSS) vulnerability. <b>REFERENCE: CVE-2017-</b> <b>2969</b>	https://helpx.a dobe.com/secur ity/products/ca mpaign/apsb17 -03.html	A-ADO- CAMPA- 280217/01
NA	15-02-2017	7.5	Adobe Campaign versions 16.4 Build 8724 and earlier have a code injection vulnerability. <b>REFERENCE: CVE-2017-</b> 2968	https://helpx.a dobe.com/secur ity/products/ca mpaign/apsb17 -03.html	A-ADO- CAMPA- 280217/02
built initially (1.x Execute Code; Overflow;			Adobe Digital Editions versions 4.5.3 and earlier	https://helpx.a dobe.com/secur	A-ADO- DIGIT-
Memory Corruption			have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. <b>REFERENCE: CVE-2017-</b> <b>2981</b>	ity/products/Di gital- Editions/apsb1 7-05.html	280217/03
Execute Code; Overflow; Memory Corruption	15-02-2017	5	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. <b>REFERENCE: CVE-2017- 2980</b>	https://helpx.a dobe.com/secur ity/products/Di gital- Editions/apsb1 7-05.html	A-ADO- DIGIT- 280217/04
Execute Code;	15-02-2017	5	Adobe Digital Editions	https://helpx.a	A-ADO-
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

CV Scoring Scale0-11-22-33-44-55-				5-6	6-7	7-8		8-9	9-10				
Execute Code;	15-02-2017	5	<b>2975</b> Adobe I	Digital Edi	tions	httj	https://helpx.a		A-ADO-				
Execute Code; Overflow; Memory Corruption	15-02-2017	5	version have an memor vulnera exploita arbitran <b>REFER</b>	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful		dok ity/ gita Edi	ps://helpx be.com/sed /products/ al- tions/apsl 5.html	cur ′Di	A-AD DIGI 2802				
Execute Code; Overflow; Memory Corruption	15-02-2017	5	version have an memory vulnera exploita arbitra	2977 Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. REFERENCE: CVE-2017-		dok ity, gita Edi 7-0	https://helpx.a dobe.com/secur ity/products/Di gital- Editions/apsb1 7-05.html		A-AD DIGI 2802				
Execute Code; Overflow; Memory Corruption	15-02-2017	5	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. <b>REFERENCE: CVE-2017-</b>				https://helpx.a dobe.com/secur ity/products/Di gital- Editions/apsb1 7-05.html			Ю- Г- 17/07			
Corruption Execute Code; Overflow; Memory Corruption	15-02-2017	5	vulnera exploita arbitran <b>REFER</b> <b>2979</b> Adobe l version have an memor vulnera exploita arbitran <b>REFER</b>	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. <b>REFERENCE: CVE-2017-</b> <b>2978</b>			Editions/apsb1 7-05.html https://helpx.a dobe.com/secur ity/products/Di gital- Editions/apsb1 7-05.html			Editions/apsb1 7-05.html https://helpx.a dobe.com/secur ity/products/Di gital- Editions/apsb1 5 7-05.html			
Overflow; Memory			have an	s 4.5.3 and exploitab	ole		oe.com/sec /products/		DIGI 2802	Г- 17/05			

Overflow; Memory Corruption			versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. <b>REFERENCE: CVE-2017-</b> <b>2974</b>	dobe.com/secur ity/products/Di gital- Editions/apsb1 7-05.html	DIGIT- 280217/10
Execute Code; Overflow	15-02-2017	10	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. <b>REFERENCE: CVE-2017-</b> <b>2973</b>	https://helpx.a dobe.com/secur ity/products/Di gital- Editions/apsb1 7-05.html	A-ADO- DIGIT- 280217/11
Flash Player	ver is freewar	e softwa	are for using content created	l on the Adobe Fl	ash nlatform
			grich Internet applications, and		-
Execute Code	15-02-2017	6.8	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable type confusion vulnerability related to the MessageChannel class. Successful exploitation could lead to arbitrary code execution. <b>REFERENCE: CVE-2017-</b> <b>2995</b>	https://helpx.a dobe.com/secur ity/products/fl ash- player/apsb17- 04.html	A-ADO- FLASH- 280217/12
Execute Code	15-02-2017	6.8	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in Primetime SDK event dispatch. Successful exploitation could lead to arbitrary code execution. <b>REFERENCE: CVE-2017-</b> <b>2994</b>	https://helpx.a dobe.com/secur ity/products/fl ash- player/apsb17- 04.html	A-ADO- FLASH- 280217/13
Execute Code; Overflow; Memory Corruption	15-02-2017	10	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption	https://helpx.a dobe.com/secur ity/products/fl ash-	A-ADO- FLASH- 280217/14
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

			SDK. Su exploita arbitrar	bility in P ccessful tion could y code exe E <b>NCE: CVI</b>	l lead to ecution.	04.h	ver/apsb1 html	, -		
Execute Code	15-02-2017	10	Adobe F version earlier f use afte related Success could le executio	Flash Playe s 24.0.0.19 nave an ex r free vuln to event h ful exploit ad to arbi on. ENCE: CVI	94 and ploitable nerability andlers. cation trary code	dob ity/ ash- play 04.h	er/apsb1	cur fl	A-AD FLAS 2802	
Execute Code; Overflow	15-02-2017	10	version earlier l heap ov when pa header. exploita arbitrar	Flash Playe s 24.0.0.19 nave an ex erflow vu arsing an 1 Successfu stion could ty code exe ENCE: CVI	dob ity/ y ash-	ver/apsb1	cur fl	A-AD FLAS 2802	-	
Execute Code; Overflow; Memory Corruption	15-02-2017	10	Adobe F version earlier f memory vulnera codec (n decomp exploita arbitrar	Flash Playe s 24.0.0.19 nave an ex y corruption bility in the related to pression). So the could by code exection ENCE: CVI	dob ity/ ash- play 04.h	https://helpx.a dobe.com/secur ity/products/fl ash- player/apsb17- 04.html			0- H- 17/17	
Execute Code; Overflow; Memory Corruption	15-02-2017	10	Adobe F version earlier I memory vulnera decomp Success	Flash Playe s 24.0.0.19 nave an ex y corruption bility in the pression rooful exploit ad to arbi	94 and ploitable on he h264 outine. cation	dob ity/ ash- play 04.h	https://helpx.a dobe.com/secur ity/products/fl ash- player/apsb17- 04.html			0- H- 17/18

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

Execute Code; Overflow; Memory15-02-201710Adobe Flash Player versions 24.0.0.194 and carlier have an exploitable memory corruption vulnerability when performing garbage collection. Successful exploitation could lead to arbitrary code execution.https://helpx.a dobe.com/secur ity/products/fl ash- player/apsb17- 04.htmlA-ADO- FLASH- 280217/19Execute Code; Overflow15-02-201710Adobe Flash Player vulnerability code execution. REFERENCE: CVE-2017- 2988https://helpx.a dobe.com/secur ity/products/fl ash- player/apsb17- 04.htmlA-ADO- FLASH- 280217/20Execute Code; Overflow15-02-201710Adobe Flash Player vulnerability related to Flash Broker COM. Successful exploitation could lead to arbitrary code execution.https://helpx.a dobe.com/secur ity/products/fl ash- 04.htmlA-ADO- FLASH- 280217/20Execute Code; Overflow15-02-201710Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable in the Flash Video (FLV) odec. Successful exploitation could lead to arbitrary code execution.https://helpx.a dobe.com/secur ity/products/fl ash- player/apsb17- 04.htmlA-ADO- FLASH- 280217/21Execute Code Execute Code15-02-201710Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability in the Flash Video (FLV) odec. Successful exploitation could lead to arbitrary code execution.https://helpx.a dobe.com/secur ity/products/fl ash- player/apsb17- 04.htmlA-ADO- FLASH- 280217/21Execute Code15-02-20				execution REFER 2990	on. E <b>NCE: CVI</b>	E-2017-					
OverflowImage: Second Seco	Overflow; Memory	15-02-2017	10	version earlier memory vulnera perform collection exploita arbitran <b>REFER</b>	s 24.0.0.19 have an ex y corrupti bility whe hing garba on. Succes ation could ry code ex	94 and sploitable on en ge sful d lead to ecution.	dol ity ash pla	pe.com/ /produc i- yer/aps	secur ts/fl	FLAS	H-
OverflowImage: Second seco	,	15-02-2017	10	version earlier integer vulnera Flash B Success could le execution <b>REFER</b>	s 24.0.0.19 have an ex overflow bility rela roker COM ful exploit ad to arbi on.	dol ity, ash pla 04.	dobe.com/secur ity/products/fl ash- player/apsb17- 04.html			H-	
versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in the ActionScript 3 BitmapData class. Successful exploitation could lead to arbitrary code		15-02-2017	10	version earlier heap ov in the F codec. S exploita arbitran <b>REFER</b>	s 24.0.0.19 have an ex rerflow vu lash Video Successful ation could ry code ex	94 and ploitable lnerabilit o (FLV) d lead to ecution.	dol e ity, ty ash pla	dobe.com/secur ity/products/fl ash- player/apsb17-			H-
<b>REFERENCE: CVE-2017-</b>	Execute Code	15-02-2017	10	Adobe I version earlier use afte in the A Bitmap Success could le execution	s 24.0.0.19 have an ex r free vult ctionScrip Data class ful exploit ad to arbi on.	94 and sploitable nerability ot 3 tation trary cod	dol ity, asł pla 04.	dobe.com/secur ity/products/fl ash- player/apsb17-			H-

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

			2985						
Execute Code; Overflow	overflow				er 94 and ploitable Inerabilit der ul d lead to ecution. E <b>-2017-</b>	dobe ity/p y ash-	s://helpx.a e.com/sect products/f er/apsb17 tml	ır FLA I 280	DO- ASH- 0217/23
Execute Code	15-02-2017	10	version earlier use afte in a rou player Success could le execution	Flash Play s 24.0.0.1 have an ex- er free vult tine relate shutdown ful exploi ead to arbi on. ENCE: CV	94 and sploitable nerability ed to tation trary code	dobe ity/r ash- play 04.h	s://helpx.a e.com/sect products/f er/apsb17 tml	ır FLA I 280	DO- ISH- 1217/24
Advantech									
<i>Susiaccess</i> Advantech has m accelerate the ad									
Gain Information	13-02-2017	5	An issu Advant Server prior. A travers extract in infor	Advantech SUISAccess Server Version 3.0 and prior. An attacker could traverse the file system and extract files that can result in information disclosure. <b>REFERENCE: CVE-2016-</b>		NA d	<u> </u>	A-A SUS	DV-
Directory Traversal	13-02-2017	6	An issue was discovered in Advantech SUISAccess Server Version 3.0 and prior. The directory traversal/file upload error allows an attacker to upload and unpack a zip file. <b>REFERENCE: CVE-2016-</b> <b>9351</b>			NA	NA		DV- 51A- 9217/26
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

NA	13-02-2017	7.2	Advante Server V prior. T is store is encry key har program reverse passwo	e was disc ech SUISA Version 3. he admin d in the sy pted with d-coded in n. Attacke the admin rd for use ENCE: CV	ccess 0 and password stem and a static n the rs could n account	d I		SUS	DV- JIA- 217/27
Webaccess			, ,	C.	1				
Advantech WebA Bypass	ccess is a web l	6.4	An issue Advante Version specific locator server, able to unrestr (AUTHI BYPASS	e was disc ech WebA 8.1. By ac uniform 1 (URL) on a maliciou access pag icted ENTICATI	covered in ccess ccessing a cesource the web is user is ges ON	n NA	<u>CADA soft</u>	A-A WE	DV- BAC- 217/28
SQL Injection	13-02-2017	7.5	Advante Version exploit vulnera must su input to softwar could re adminis the app files.	e was disc ech WebA 8.1. To be the SQL ir bility, an a pply malf the Web e. Success esult in strative ac lication an ENCE: CV	ccess e able to ajection attacker formed Access aful attack ccess to ad its data	ζ		WE	DV- BAC- 217/29
Artifex									
<i>Mupdf</i> MuPDF is a free and EPUB parsing	-			amework	written	in C tha	t implen	ients a	PDF, XPS,
Denial of	15-02-2017	4.3	Heap-b	ased buffe	er	https	s://bugs.g	gh A-A	RT-
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Service; Overflow			fz_subs function MuPDF remote denial o bounds a crafte	w in the ample_pix n in fitz/p 1.10a allo attackers of service read and d image. ENCE: CV	ixmap.c i ows to cause (out-of- crash) vi	n = a		ript.com bug.cgi? 515		MUP 2802	DF- 17/30
Denial of Service	15-02-2017	4.3	The pdf pdf-obj before attacke of servi and app crafted	f_to_num f ect.c in Mu 1.10 allow rs to cause ce (use-af olication c file. ENCE: CV	uPDF vs remote e a denial ter-free rash) via	: ( [	redh	//bugzi at.com/s ug.cgi?ic 685	sh	A-AR MUP 2802	
NA	15-02-2017	5	An issue was discovered in Artifex Software, Inc. MuPDF before 1912de5f08e90af1d9d0a9 791f58ba3afdb9d465. The pdf_run_xobject function in pdf-op-run.c encounters a NULL pointer dereference during a Fitz fz_paint_pixmap_with_mas k painting operation. <b>REFERENCE: CVE-2017-</b>				ostsc	ript.com bug.cgi?	/s	A-AR MUP 2802	
Atutor										1	
<i>Atutor</i> ATutor is a free adaptability in mi	•	ce Learr	ning Mar	nagement	System	des	igneo	l with	acc	essibil	ity and
Execute Code; Cross Site Request Forgery	07-02-2017	6.8	(CSRF) install_ ATutor remote the aut for requ arbitra	ite reques vulnerabi modules.p before 2.2 attackers henticatio uests that ry files and ry PHP coo	5 ( 5 ( 5 ( 5 (	https://github.c om/atutor/ATu tor/commit/bfc 6c80c6c217c55 15172f3cc949e 13dfa1a92ac			ATUTO- 280217/33		
CV 0-1	1-2	2-3	3-4	4-5	5-6		-7	7-8		8-9	9-10

	vectors involvin zip file. <b>REFERENCE: C</b>										
			2539		2010						
Autotrace Proje	ct					•					
Autotrace											
Autotrace is a pro	ogram which co 15-02-2017	onverts l	oitmap in	nages to ve	ector ima	ges.					
Denial of Service; Overflow	4.3	pstoedi function pstoedi 0.31.1 a attacke of servi write) v image f	overflow in the pstoedit_suffix_table_init function in output- pstoedit.c in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted bmp image fileredhat.com/sh ow_bug.cgi?id= 1375255AutoTrace 13752551375255AutoTrace 						A-AU 		
Bigtreecms											
Bigtree Cms											
BigTree CMS is an	n open source (	content	nanagem	lent syster	n built or	ו PHP	P and	l MySQL			
Execute Code	14-02-2017	3.5	An issue was discovered in BigTree CMS before 4.2.15. The vulnerability exists due to insufficient filtration of user-supplied data in the "id" HTTP GET parameter passed to the "core/admin/adjax/dashbo ard/check-module- integrity.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website. <b>REFERENCE: CVE-2016-</b> <b>10223</b>				ttps: m/b BigT MS/	://githul igtreecn	o.c 1s 1st	A-BIO BIGT 2802	
Bubblewrap Pro	ject										
<b>Bubblewrap</b> Bubble Wrap is a isBubbleWrap.ex		loped by	y XM Asia	Pacific Pt	e Ltd. The	e mai	in pr	ogram e:	xecı	ıtable	
Gain Privileges	13-02-2017	6.9	Bubble sets the	wrap befo	re 0.1.3		-	://githul rojectate		A-BU BUBE	
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8		8-9	9-10

BusyboxREFERENCE: CVE-2016- 8659Busybox09-02-20175Denial of Overflow09-02-20175Integer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to out-of-bounds heap write. REFERENCE: CVE-2016- 2147https://git.busy box.net/busybo ada651c4432e eabfa62cd51e8Overflow09-02-20177.5Heap-based buffer out-of-bounds heap write. REFERENCE: CVE-2016- 2147https://busybo cause a denial of service (crash) via a malformed name, which triggers an out-of-bounds heap write. REFERENCE: CVE-2016- 2147https://busybo A-BUS- BUSYB- 280217/38Overflow09-02-20177.5Heap-based buffer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to have unspecified impact via vectors involving OPTION.6RD parsing. REFERENCE: CVE-2016- 2148https://busybo A-BUS- BUSYB- 280217/38Cairor sa 2D graphics library with support for multiple output devices. Denial of Service; Overflow03-02-20174.3Integer overflow in the write_ping function in cairo of service (invalid pointer dereference) via a large svg file. REFERENCE: CVE-2016- 2148https://busybo A-CAI- desktop.org/at CAIRO- 280217/39	CV Scoring	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Busyboxattaching to the process, as demonstrated by sending commands to a PrivSep socket. 	<b>Cairo</b> Cairo is a 2 Denial of Service;	D graphic			Integer write_p 1.14.6 a attacke of servi derefer file. <b>REFER</b>	overflow ng functio illows rem rs to cause ce (invalio ence) via a	in the on in cairc note e a denial d pointer a large sv	http edes tach =12	sktop.org/ ment.cgi?	at CAII	R0-
BusyboxREFERENCE: CVE-2016- 8659https://git.busy 8002.101A-BUS- 8002.101BusyboxInteger overflow in the BusyBox is a software that provides several stripped-down Unix tools in a single executable file.https://git.busy 8002.101A-BUS- 8002.101Denial of Service; Overflow09-02-20175Integer overflow in the BusyBox before 1.25.0 allows remote attackers to (crash) via a malformed (Crash) via a malformed RFFERENCE: CVE-2016- 2147https://git.busy 8003651c4432e eabfa62cd51e8 7A-BUS- 803651c4432e eabfa62cd51e8 7Overflow09-02-20177.5Heap-based buffer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to have unspecified impact via vectors involving OPTION_6RD parsing.https://busybo A-BUS- 280217/38	Cairograp	hics									
attaching to the process, as     demonstrated by sending     commands to a PrivSep     socket.     REFERENCE: CVE-2016-     8659	Denial of Service; Overflow	0	9-02-2017	5	Integer DHCP c BusyBo allows r cause a (crash) RFC103 name, v out-of-l <b>REFER</b> 2147 Heap-b overflor (udhcp 1.25.0 a attacke unspec: vectors OPTION	overflow lient (udh x before 1 cemote att denial of via a malf 5-encode vhich trigg bounds he ENCE: CVI ased buffe w in the D c) in Busy llows rem rs to have ified impa involving V_6RD par	in the cpc) in 25.0 tackers to service formed d domain gers an ap write. <b>E-2016</b> - er HCP clier Box befor note ct via	http box. x/cc 0 d47 0a8 eabf 7 http t. x.ne	s://git.bu net/busyk ommit/?id 4ffc68290 3651c443 2a62cd51e s://busyb	sy A-BI bo BUS = 280 e 2e 8 8 m BUS	US- YB- 217/37 US- YB-
attaching to the process, as demonstrated by sending commands to a PrivSep socket. REFERENCE: CVE-2016- 8659	Busybox	a softwa	re that pro	vides seve	eral strin	ned-dowr	Unix too	ls in a s	ingle exec	utable fil	<u></u>
PR_SET_DUMPABLE flag, mic/bubblewra 280217/36 which might allow local p/issues/107					which r users to attachin demons comma socket. <b>REFER</b>	night allow gain priv ng to the p strated by nds to a P	w local vileges by process, as sending rivSep	p/is		ra 280.	217/36

Chatsecure;ZOM	[				
Chatsecure/ZOM	I				
ChatSecure is a fr	ee and open so	urce me	essaging app that features OT	R encryption over 2	XMPP/ Zom is
the next generati	on communicat	ion app	based on ChatSecure focused	on hyper usability.	
NA	09-02-2017	4.3	An incorrect implementation of "XEP- 0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for ChatSecure (3.2.0 - 4.0.0; only iOS) and Zom (all versions up to 1.0.11; only iOS). <b>REFERENCE: CVE-2017-</b>	NA	A-CHA- CHATS- 280217/40
Cisco			5590		
collaboration, on Meeting Center p	ormerly WebE line meeting, v rovides cost-ef	x Comi web cor fective e	er nunications Inc. is a comp nferencing and videoconferen enterprise video conferencing; aboration and communication	icing applications; Cisco WebEx Mee	Cisco WebEx tings Server is
Execute Code; Overflow	01-02-2017	9.3	An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. Vulnerability in these Cisco WebEx browser	https://tools.cis co.com/security /center/content /CiscoSecurityA dvisory/cisco- sa-20170124- webex	A-CIS- ACTIV- 280217/41
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

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

Cisco Prime Hom Cisco Prime Hom solution that pro	ne provides a		due to i implem access could e vulnera the Inte browse allow th Interne privileg user. Th attacke privileg the targ vulnera version later ar later. C CSCvc4 <b>REFER</b> <b>3813</b>	ENCE: CVI	t of the an attacke opening orer oit could r to use with the SYSTEM low the te ands on em. This cts released 43 and 17 and Ds: E-2017-	ote man			
subscriber experi Execute Code; Bypass	01-02-2017	10	based ( Home of unauth attacke authen actions privileg vulnera process role-ba (RBAC) attacke vulnera API cor a partio	ability in the GUI of Cisc could allow enticated, or to bypas tication and with adm ges. The ability is du sing error sed access of URLs. A r could ex ability by so nmands vi cular URL uthenticat could allo	o Prime v an remote s ad execute inistrator ue to a in the s control An ploit this sending a HTTP to without ion. An	co.co /cen /Ciso dviso e sa-20 prim	s://tools. om/secur ter/conte coSecurit ory/cisco 0170201- e-home	ity CIS ent 28 yA -	CIS- GCO- 0217/43

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

attacker to perform any actions in Cisco Prime Home with administrator privileges. This vulnerability affects Cisco Prime Home versions from 6.3.0.0 to the first fixed release 6.5.0.1. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. Cisco Bug IDs: CSCvb49837.	
REFERENCE: CVE-2017- 3791	

## Firepower Management Center

The Cisco Firepower Management Center (formerly FireSIGHT Management Center) is the administrative nerve center for select Cisco security products running on a number of different platforms.

S- P- 217/44
, ,
5-
р-
r- 217/45
.1//45

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

			6.2.0. Ki Release	Releases nown Fixe s: 6.1.0.1 ENCE: CV	ed 6.2.0.					
Prime Service Ca Cisco Prime Serv		widos a	colf-com	ico port	l corvic	-roque	et manage	mon	ut and	an IT
service catalog fo	<b>U</b> .			-		-icque	st manage	men	n, anu	
NA	03-02-2017	4.9	Vulnera framew Service an autho attacker URL red a user w an affec Informa Known 2	bility in t ork of Cis Catalog c enticated to condu irect atta who is logated ted system	co Prime ould allow , remote act a web ck agains ged in to m. More vb21745. Releases: a.	v /ce /Ci dvi t sa- psc	ps://tools. com/secur enter/conte scoSecurity sory/cisco 20170201-	ity ent yA -	A-CIS- PRIME 28021	
Telepresence Mc				c.						
The Cisco TelePre that can grow wit				-	e-of-the-a	rt mult	cipoint cont	trol ı	units (M	ACUs)
Denial of Service; Execute Code; Overflow	01-02-2017	10	Vulnera propriet in the ke TelePre Control Softwar unauthe attacker arbitrar denial o condition is due to validation reasser IPv4 or attacker vulneration crafted 1 fragmer receivin Passthro	bility in a cary device ernel of C sence Mu Unit (MC e could al enticated, to execu y code or f service on The vu o imprope on when bling frag IPv6 pack could ex bility by s iPv4 or IF ats to a po g content ough content	ce driver isco ltipoint U) low an remote te cause a (DoS) lnerabilit er size gmented cets. An ploit this sending Pv6 ort c in cent mode	co.d /ce /Ci dvi sa- tele	ps://tools. com/secur nter/conte scoSecurity sory/cisco 20170125- epresence	ity ent yA -	A-CIS- TELEP 28021	7/47
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	<b>9-1</b> 0

			attacke buffer. attacke arbitran DoS con affected TelePre platforn MCU 53 TelePre	oit could a r to overfl If successf r could ex ry code or ndition on l system. ( esence MC ms TelePr 800 Series esence MC nd TelePre	ow a Ful, the ecute cause a the Lisco U esence , U MSE						
			when reversion configut content release that add vulnerat availab are ava IDs: CS	500 are aff unning so 4.3(1.68) red for Pa mode. Cis d software dress this bility. Wo dress this bility are le, but mit ilable. Cise Cuu67675 ENCE: CV	ftware or later ssthrougl sco has e updates rkaround not igations co Bug						
<b>Unified Computin</b> Cisco UCS Directo				anageme	nt solutio	n th	nat m	akes it	easi	er to	manage
Vblock, FlexPod, a	and VSPEX envi	ironmen	its.							I	_
NA	15-02-2017	4.6	based C Directo could a authent attacke arbitrat with jus profile, Escalat The vul improp control Develop	ability in t UI of Cisc r 6.0.0.0 a llow an ticated, loo r to execu ry workflo st an end- a Privileg ion Vulner nerability er role-ba (RBAC) a per Menu	o UCS nd 6.0.0.1 cal te w items user e rability. r is due to sed acces fter the is enableo		co.con /cent /Cisco dviso	://tools. m/secur er/contro oSecurit ry/cisco 170215	rity ent zyA )-	A-CIS UNIF 2802	
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6	-7	7-8		8-9	9-10

			vulnera Develop his/her end-use adding arbitran to his/h exploit attacke actions workflo actions tenants CSCvb6	r could ex ability by e per Mode t user profile a new catale ry workflo ner profile could allo r to perfor defined b ow items, i affecting c. Cisco Bu 4765. ENCE: CV	enabling for ile with a and then ogs with w items . An w an cm any y these including other g IDs:	n				
Conversejs										
<i>Converse.js</i> Converse.js is a fi	ree and onen-	source XN	MPP chat	client in v	our brow	vser				
NA	09-02-2017	4.3	An inco implem 0280: M multipl allows a includin vulnera display various enginee CVE is f (0.8.0 -		of "XEP- arbons" in ients attacker t user, s, in the cation's ws for social eks. This se.js 0 - 2.0.4).	NA n o			A-CO CONV 2802	
<b>Dhcpcd Project</b>										
<b>Dhcpcd</b> dhcpcd is an imp and RFC1541 (w) Denial of Service; Overflow			ed). dhcpcd allows cause a	specified i before 6.1 remote att denial of 1 l read and	10.0 cackers to service	htt les ts/	p://roy.ma name/pro dhcpcd/in 95883e2a4	arp jec fo 3	A-DH DHCI	C-
			vectors option	related to	o the		5d8fabf33 4689cca1			
			option	iengui.		700	TUUTUAL	/ 4		
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

			DEEDD		0.047				
			REFER 1504	ENCE: CV	E-2016-	03			
Dotclear			1304						
Dotclear									
Dotclear is an op	en source blog i	oublishi	ng applic	ation dist	ributed u	nder the	GNU GPL	/2.	
Cross Site Scripting	09-02-2017	4.3	Cross-s vulnera admin/ Dotclea allows i inject a or HTM name ir	ite scripti bility in comment r before 2 remote att rbitrary w L via the a a comme ENCE: CV	A-DOT- DOTCL- 280217/51				
Execute Code	ecute Code 09-02-2017 6.5				ete pilities in core.php e 2.8.2 henticated ge their " and vn entries kecute de by vith a (1) (3) .phtm E-2015-	ear.c r/rev c3d8 d	s://hg.doto org/dotclea v/1985801	a DOT	
Dotcms			•					<b>I</b>	
<b>Dotcms</b> dotCMS is a open content driven w	eb apps and sit	es.					r managin		
Cross Site Scripting	06-02-2017	3.5	dotCMS authent against address	s discover 3.7.0, wit cicated att the /myA SID param ENCE: CV	h an ack ccount eter.	NA		-	0T- `CM- 217/53
Cross Site Scripting	06-02-2017	4.3	dotCMS	s discover 3.7.0, wit enticated	h an	NA			OT- `CM- 217/54
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			against the /about- us/locations/index direction parameter. <b>REFERENCE: CVE-2017-</b> <b>5877</b>		
Cross Site Scripting	06-02-2017	4.3	XSS was discovered in dotCMS 3.7.0, with an unauthenticated attack against the /news- events/events date parameter. <b>REFERENCE: CVE-2017-</b> <b>5876</b>	NA	A-DOT- DOTCM- 280217/55
Dotnetnuke					
<b>Dotnetnuke</b> DNN (formerly D	otNetNuke) is a	a web co	ntent management system ba	sed on Microsoft .N	IET.
NA	06-02-2017	7.5	The installation wizard in DotNetNuke (DNN) before 7.4.1 allows remote attackers to reinstall the application and gain SuperUser access via a direct request to Install/InstallWizard.aspx. <b>REFERENCE: CVE-2015-</b> <b>2794</b>	http://www.dn nsoftware.com/ community- blog/cid/15519 8/workaround- for-potential- security-issue	A-DOT- DOTNE- 280217/56
EMC					
<i>Isilon Insightiq</i> EMC Isilon data i and system perfo	-	ftware p	rovides you with powerful to	ols to optimize stor	age resources
Bypass	08-02-2017	7.5	EMC Isilon InsightIQ 4.1.0, 4.0.1, 4.0.0, 3.2.2, 3.2.1, 3.2.0, 3.1.1, 3.1.0, 3.0.1, 3.0.0 is affected by an authentication bypass vulnerability that could potentially be exploited by attackers to compromise the affected system. <b>REFERENCE: CVE-2017-</b> <b>2765</b>	http://www.sec urityfocus.com/ archive/1/5401 00/30/0/threa ded	A-EMC- ISILO- 280217/57
Exponentcms					
Exponent Cms	•	irce Coi	ntent Management System, h	oased on PHP, M	ySQL and the
CV Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

SQL Injection	06-02-2017	7.5	An issue was discovered in Exponent CMS 2.4.1. This is a blind SQL injection that can be exploited by un- authenticated users via an HTTP GET request and which can be used to dump database data out to a malicious server, using an out-of-band technique, such as select_loadfile(). The vulnerability affects source_selector.php and the following parameter: src. <b>REFERENCE: CVE-2017- 5879</b>	NA	A-EXP- EXPON- 280217/58
Execute Code; SQL Injection	07-02-2017	7.5	Multiple SQL injection vulnerabilities in Exponent CMS before 2.4.0 allow remote attackers to execute arbitrary SQL commands via the (1) id parameter in an activate_address address controller action, (2) title parameter in a show blog controller action, or (3) content_id parameter in a showComments expComment controller action. <b>REFERENCE: CVE-2016-</b> 7400	https://github.c om/exponentc ms/exponent- cms/commit/e 916702a91a63 42bbab483a2b e2ba2f11dca3a a3	A-EXP- EXPON- 280217/59
Execute Code	13-02-2017	7.5	install/index.php in Exponent CMS 2.3.9 allows remote attackers to execute arbitrary commands via shell metacharacters in the sc array parameter. <b>REFERENCE: CVE-2016-</b> <b>7565</b>	https://expone ntcms.lighthous eapp.com/proje cts/61783/cha ngesets/4ae457 ff1bf80e8b6128 6cd125ca794b2 5564e86	A-EXP- EXPON- 280217/60
Fatek					
<b>Automation Fv D</b> Fv Designer is a s	· · · · · · · · · · · · · · · · · · ·		<b>Pm Designer</b> esign and develop FATEK FV	HMI series produc	t projects; PM

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

Designer is the pr	rogram used to	edit the	e settings of Fatek HMI hardware.						
Overflow	13-02-2017	5	An issue was discovered in Fatek Automation PMNAA-FAT- AUTOM- 280217/61Designer V3 Version280217/612.1.2.2, and Automation FV Designer Version 1.2.8.0.8By sending additional valid packets, an attacker could trigger a stack-based buffer overflow and cause a crash. Also, a malicious attacker can trigger a remote buffer overflow on the Fatek Communication Server.Here REFERENCE: CVE-2016- 5798						
Execute Code; Overflow	13-02-2017	6.8	An issue was discovered in Fatek Automation PM Designer V3 VersionNAA-FAT- AUTOM- 						
Ffmpeg									
<i>Ffmpeg</i>	coftware projec	t that n	roduces libraries and programs for handling multimedia data.						
Execute Code; Overflow09-02-20177.5Heap-based buffer overflow in ffserver.c in FFmpeg before 2.8.10, 3.0.x before 3.0.5, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 allows remote attackers to execute arbitrary code by leveraging failure to check chunk size.https://ffmpeg. org/security.htA-FFM- FFMPE- 280217/63REFERENCE: CVE-2016- 1019210192101921019210192101921019210192									
CV Scoring Scale	1-2	2-3	3-4     4-5     5-6     6-7     7-8     8-9     9-10						

			2.40.2 a attacke of servi read) v	erver.c in Illows ren rs to caus ce (out-of a a crafte ENCE: CV	note e a denial -bounds d svg file.		53520			
GNU										
Libiberty										
The libiberty libr										
Denial of Service; Overflow	07-02-2017	5	Libiber attacke of servi stack ov via a cy of reme types.	nangler ir ty allows i rs to cause ce (infinit verflow, ai cle in the mbered n ENCE: CV	remote e a denial e loop, nd crash) reference nangled	org ow 710	ps://gcc.gn g/bugzilla/s _bug.cgi?id 596	sh	A-GN LIBIB 2802	
Gosa Project			•					<u> </u>		
Gosa Plugin GOsa is a combin based setups. Cross Site Scripting Gradle	ation of system	a-admin	Cross-s vulnera display html/in allows i inject a or HTM	ite scripti bility in the Login fund dex.php i remote att rbitrary w L via the u ENCE: CV	htt om pro cor 35l 2cf	ce, designed ps://githuk /gosa- oject/gosa- ce/commit/ o990464a2 64d6833a2 1944876e7	o.c /e 21	A-GO	e LDAP S-GOSA 217/69	
Gradle										
Gradle is the next	t evolutionary s	tep in IV	/M-based	build too	ols.					
Execute Code	07-02-2017	7.5	ObjectS in Grad remote arbitran serializ	ObjectSocketWrapper.java in Gradle 2.12 allows remote attackers to execute arbitrary code via a crafted serialized object. <b>REFERENCE: CVE-2016-</b>					A-GR GRAD 2802	
Gstreamer Proje	ect									
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8.	-9	9-10

Gstreamer			
			edia framework that links together a wide variety of media
	ems to complete		
Denial of Service	09-02-2017	4.3	Thehttps://gstreamA-GST-gst_asf_demux_process_ext_er.freedesktop.oGSTRE-stream_props function inrg/releases/1.1280217/71gst/asfdemux/gstasfdemux0/#1.10.3///////////////////////////////
Denial of Service	09-02-2017	4.3	The gst_riff_create_audio_caps function in gst- libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 allows remote attackers to 
Denial of Service	09-02-2017	4.3	Thehttps://gstreamA-GST-html_context_handle_elemeer.freedesktop.oGSTRE-nt function inrg/releases/1.1280217/73gst/subparse/samiparse.c0/#1.10.30/#1.10.3in gst-plugins-base inGStreamer before 1.10.310/#1.10.3GStreamer before 1.10.3allows remote attackers toacause a denial of service(out-of-bounds write) via acrafted SMI file, as4demonstrated byOneNote_Manager.smi.REFERENCE: CVE-2017-584258425
Denial of	09-02-2017	4.3	The https://gstream A-GST-
CV Scoring Scale	-1 1-2	2-3	3-4     4-5     5-6     6-7     7-8     8-9     9-10

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	3-9	9-10
Denial of Service	0	9-02-2017	5	content gst/asfo .c in gst GStrear	demux_pi _desc fund lemux/gs -plugins-u ner allows rs to cause	ction in tasfdemu ıgly in s remote	t_ om/ gst-j x ugly 210 145	s://githul GStreame plugins- /commit/ 17b52a58 e8d62781 :5fefc7ee3	er/ /d 85f .b	A-GS GSTF 2802	
Denial of Service	0	9-02-2017	5	function gst/mp emux.c in GStre remote denial c memory via vect parsing	egdemux/ in gst-plu eamer allo attackers of service y read and ors involv	/gstmpeg gins-bad ws to cause (invalid l crash) ving PSM	.gno w_b d 779	s://bugzi me.org/sl ug.cgi?id= 57#c3	10	A-GS GSTF 2802	
Denial of Service		9-02-2017		function gst/aud rse.c in GStrear allows n cause a (invalid crash) v file. <b>REFER</b> <b>10198</b>	_parse_sin n in lioparsers gst-plugin ner before remote att denial of memory via a crafte ENCE: CV	/gstaacpa ns-good ir 2 1.10.3 cackers to service read and ed audio	s er.fr rg/r a 0/#	s://gstrea eedesktoj eleases/1 1.10.3	p.o .1		RE- 17/75
Service				function libs/gst gst-plug GStrear allows n cause a (floatin and cra video fi	/riff/riff- gins-base ner before remote att denial of g point ex sh) via a c	media.c ir in 2 1.10.3 cackers to service ception rafted	rg/r n 0/#	eedesktoj eleases/1 1.10.3		GSTF 2802	RE- 17/74

				via vect	ors involv	ing ncdt					
Denial of Service	0	9-02-2017	7 5	function gst/avi, gst-plug GStrear allows n cause a (out-of-	/gstaviden gins-good ner before remote att denial of s bounds he	nux.c in in 1.10.3 ackers to service eap read)	er.fre rg/re	s://gstrea eedesktop eleases/1 10.3	<b>p.o</b>	A-GST GSTRI 28021	
Denial of Service		9-02-2017		5845Multiplevulneragst_mingst_tag_gst_tag_gst_mxfence_traGStrearallow recause a(crash)involvindemons027857REFER5843	e use-after bilities in i_object_u list_unref, _demux_u acks funct ner before emote atta denial of s via vector ng stream strated by	r-free the (1) nref, (2) and (3) pdate_ess ions in 1.10.3 ckers to service s tags, as	er.fre rg/re 0/#1	s://gstrea eedesktop eleases/1 10.3	p.o .1		E- L7/79
Denial of Service	0	9-02-2017	7 5	heap re involvin descrip <b>REFER</b> <b>5847</b> The gst_avi_ function gst/avi, gst-plug GStrear allows n cause a (invalid crash) v that "go	ENCE: CVE	ctors ed content <b>E-2017-</b> arse_ncdt nux.c in in 1.10.3 ackers to service read and sub-tag " the	https er.fre rg/re	s://gstrea eedesktop eleases/1 10.3	<b>p.o</b>	A-GST GSTRI 28021	

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

				tags. <b>REFER</b> <b>5841</b>	ENCE: CVI	E-2017-						
Denial of Service	09-(	02-2017	5	The qtdemu function gst/ison gst-plug GStrear allows n cause a (out-of- via vect current <b>REFER</b> 5840	er rg 0/	https://gstream er.freedesktop.o rg/releases/1.1 0/#1.10.3			GSTRE- 280217/81			
Denial of Service; Overflow	09-02-2017 5 The gst_riff_create_audio_caps function in gst- libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 does not properly limit recursion, which allows remote attackers to cause a denial of service (stack overflow and crash) via vectors involving nested WAVEFORMATEX. <b>REFERENCE: CVE-2017-</b>					er rg n 0/	https://gstream er.freedesktop.o rg/releases/1.1 0/#1.10.3			GSTRE- 280217/82		
Denial of Service	09-(	02-2017	5	o8601_ gst/gsto GStrear allows r cause a (out-of- via a ma string.	e_time_nev string fund datetime.c ner before remote att denial of s bounds he alformed c ENCE: CVI	ction in in 2 1.10.3 ackers to service eap read) latetime	s er rg 0/	.free	//gstre edeskto eases/1 10.3	p.o	A-GS GSTF 2802	
Denial of Service	09-0	02-2017	5	The	x_tag_add	_str_full		-	//gstre edeskto		A-GS GSTF	
				-								

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	<b>9-1</b> 0
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	--------------

			function in gst/isomp4/qtdem gst-plugins-good in GStreamer before 2 allows remote atta- cause a denial of se (out-of-bounds rea crash) via a crafted value. <b>REFERENCE: CVE-</b> 10199	1 1.10.3 ckers to ervice d and tag	rg/releases/1.1 0/#1.10.3	280217/84		
Guac-dev								
Guacamole								
Guacamole is a pr	rogram to contr	ol a Lin	ix desktop over the	network i	n a browser.			
Cross Site Scripting	02-02-2017	3.5	Cross-site scripting vulnerability in the browser in Guacam 0.9.8 and 0.9.9, who transfer is enabled location shared by users, allows remo authenticated user inject arbitrary we or HTML via a craft filename. NOTE: th vulnerability was fi guacamole.war on 01-13, but the vers number was not ch <b>REFERENCE: CVE-</b> <b>1566</b>	g (XSS) e file nole en file to a multiple te s to b script ted nis ixed in 2016- ion anged.	https://sourcef orge.net/p/gua camole/news/2 016/02/securit y-advisory stored-xss- Reference: CVE 2016-1566 guac-1465/	GUACA- 2 280217/85		
Hanwha Techwi	n							
of Wisenet IP ne third party syster Execute Code;	s a one-stop, tot twork cameras	s, record	management softw ling devices and se ms and Access Cont An issue was disco	rvers, wh rol. vered in	ilst facilitating i https://ics-	A-HAN-		
Cross Site Request Forgery	s Site Hanwha Techwin Smart cert.us- SMART Security Manager Versions cert.gov/adviso 280217							
CV Scoring Scale	1-2	2-3	3-4 4-5	5-6	6-7 7-8	8-9 9-10		

CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
depth granularit customers detern Gain Information	y across all o	devices;	IBM Lie capacity j IBM Bi	cense Me	tric Tool value unit ntory v9	helps <mark>s (PVU</mark> http	IBM Pas	sport A grequire o A-II	dvantage ements. 3M-
Bigfix Inventory; IBM BigFix Inven embedded compl	tory provides	the foun					-	-	
IBM			executi						
Execute Code; Directory Traversal	13-02-2017	5.1	for rem <b>REFER</b> <b>5169</b> An issu Hanwha Security 1.5 and Travers have be flaws ex Active that is i the pro specific user vis an attact to arbit server. Manage prior to by thes These v allow for execution	e was disc a Techwin y Managen prior. Mu cal vulnera en identif kist withir IQ Broker nstalled a duct. By is HTTP rec sits a malie cker can g rary files Smart Sec er Version 1.31 are a e vulnerabilio pr remote on.	execution. E-2017- covered in a Smart Versions ltiple Path abilities fied. The a the service s part of suing quests, if a cious page ain access on the curity s 1.4 and affected pilities. ties can code	cert. cert. ries, 040·	gov/advis /ICSA-17-	SMA	AN- ART- 217/87
			this pro specific request gain sys a remot Smart S Version affected vulnera	duct. By i HTTP Po- s, an attac stem level e shell se ecurity M s 1.5 and l by these bilities. T	st cker can access to ssion. anager prior are hese				

			stored locally which can be read by another user on the system./docview.wss?u id=swg2199493280217/88REFERENCE: CVE-2016- 8981211
NA	01-02-2017	2.1	IBM BigFix Inventory v9http://www.ibA-IBM-9.2 stores user credentialsm.com/supportBIGFI-in plain in clear text which/docview.wss?u280217/89can be read by a local user.id=swg21995019 <b>REFERENCE: CVE-2016-</b> 99
Gain Information	01-02-2017	2.1	IBM BigFix Inventory v9 stores potentiallyhttp://www.ib m.com/supportA-IBM- BIGFI- 
Gain Information	01-02-2017	4.3	IBM BigFix Inventory v9 could allow a remote attacker to obtainhttp://www.ib m.com/support 
Gain Information	01-02-2017	5	IBM BigFix Inventory v9 could disclose sensitive information to an unauthorized user using 
Gain Information	01-02-2017	5.8	IBM BigFix Inventory v9http://www.ibA-IBM-could allow a remotem.com/supportBIGFI-attacker to conduct/docview.wss?u280217/93
CV 0- Scoring Scale	1 1-2	2-3	3-4     4-5     5-6     6-7     7-8     8-9     9-10

Denial of Service01-02-20177.5IBM BigFix Inventory v9 is vulnerability logton (XXE) error when processing XML data. A remote attacker could al available memory resources.http://www.ib BIGFI- BV80A-IBM- BIGFI- 28021Denial of Service01-02-20177.5IBM BigFix Inventory v9 is vulnerability to spose highly sensitive information or conduct further attacks against the victim.http://www.ib m.com/support BIGFI- 28021Denial of Service01-02-20177.5IBM BigFix Inventory v9 is vulnerability information or conduct further attacks against the victim.http://www.ib m.com/support 3A-IBM- BIGFI- 28021
---

## **Bigfix Platform**

IBM BigFix formerly IBM Endpoint Manager, Tivoli Endpoint Manager (TEM) and before that, BigFix, is a systems-management software product developed by IBM for managing large groups of computers running Windows, Mac OS X, VMware ESX, Linux or UNIX, as well as various mobile operating systems such as Windows Phone, Symbian, iOS and Android.

NA	01-02-2017	2.1	IBM Tivoli Endpoint	http://www.ib	A-IBM-
			Manager - Mobile Device	m.com/support	BIGFI-
			Management (MDM)	/docview.wss?u	280217/95
			stores potentially	id=swg2199321	
			sensitive information in	3	
			log files that could be		
			available to a local user.		
			<b>REFERENCE: CVE-2016-</b>		

			0296								
NA	01-02-2017	3.3	allow a local n BES ar	gFix Platf an attacke etwork to nd relay se <b>RENCE: CV</b>	m.co /doc	//www.i m/suppo view.wss vg21996	ort s?u	A-IB BIGF 2802			
NA	01-02-2017	3.3	allow a local n BES se specia XMLSc	gFix Platf an attacke etwork to rver using lly crafted chema req <b>RENCE: CV</b>	r on the crash the g a uest.	e	m.co /doc	//www.i m/suppo view.wss vg21996	ort s?u	A-IB BIGF 2802	
Gain Information	01-02-2017	4.3	Manag Manag allow a obtain inform missin Transp Heade the mi	voli Endp ger - Mobil gement (M a remote a sensitive ation due g HTTP St port-Secur r through ddle techr <b>RENCE: CV</b>	e Device DM) coul attacker t to a crict- rity man in niques.	0	m.co /doc	//www.i m/suppo view.wss vg21993	ort s?u	A-IB BIGF 2802	
Execute Code	01-02-2017	6.8	Manag user u circum comma execut unnece privile	voli Endp ger could a nder speci astances to ands that ed with essary hig ges than e <b>RENCE: CV</b>	llow a ial o inject would be her expected.		m.co /doc	//www.i m/suppo view.wss vg21993	ort s?u	A-IB BIGF 2802	
NA	08-02-2017	6.8	IBM Ti Manag remoto arbitra attacko vulner malicio	voli Endp ger could a e attacker ary files. A er could ez ability to pous file. Th at file wor	llow a to upload remote xploit thi upload a ne only		m.co /doc	//www.i m/suppo view.wss vg21993	ort s?u	A-IB BIGF 2802	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6		6-7	7-8		8-9	9-10

CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7	-8	8-9	9-10
Cross Site Scripting	01-02-2017	3.5	BigInsi to cros caused validat input. <i>J</i> could e vulner special execut	fosphere ghts is vu s-site scri by impro ion of use A remote exploit thi ability usi ly-crafted e script in rowser wi	pting, oper artsupplie attacker s ng a l URL to a victim'	m. /d id= d 9	tp://ww com/su ocview =swg21	ipport .wss?u		
<b>Biginsights</b> BigInsights is a Platform with Ap Cross Site Scripting			he open IBM In BigInsi to cros This vu users t JavaSc UI thus intend potent creden within		oundation lnerable pting. cy allows arbitrary in the We the onality ng to osure session.	1. htt m. /d id= 9	ed on t tp://ww com/su ocview =swg21	ww.ib ipport .wss?u	A-IB BIGI 2802	M-
Execute Code	01-02-2017	10	throug to trick victim <b>REFER</b> <b>0214</b> IBM Bi allow a execut the sys use-aft could e vulner arbitra system	ed would h a phishi c an unsus to execute ENCE: CV gFix Platfo remote a e arbitrary tem, caus er-free ra ion. An att exploit thi ability to o ry code of the ENCE: CV	ng attack specting e the file. <b>TE-2016-</b> orm could attacker to y code on ed by a ce cacker s execute n the	l htt o m. /d	tp://wv com/su ocview =swg21	ipport .wss?u		

Business Process Manager is a full-featured, consumable business process management (BPM platform.     Cross Site   01-02-2017   3.5   IBM Business Process Manager is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. REFERENCE: CVE-2016-9731   A-IBM-BUSIN-280217/10     Campaign     Campaign     Compaign     Drovides multichannel marketing campaign management.     Cross Site     OI-02-2017     Scripting     Campaign     Drovides multichannel marketing campaign management.     Cross Site     OI-02-2017     Scripting     Cross Site     Scripting     Scripting
--

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

			0265							
<b>Client Applicatio</b>	n Access; Dom	ino; Note	es							
IBM Client Applie solution for access Domino) is an ad Notes, is an ent	cation Access ( sing your IBM vanced platfor	(formerly Notes an m for ho	v known d IBM D sting so	omino apj cial busin	olications; ess applic	IBM Do ations;	omino (foi IBM Note	rme s, fo	erly IB	M Lotus y Lotus
collaboration. Gain	08-02-2017	4.3	IRM D	omino 9.0	1 Fix Daci	z http	://www-		A-IBI	<u>И_</u>
Information	08-02-2017	4.3	3 Inter 9.0.1 F Fix 1, x AES GO nonce makes attack auther spoof o the reu session attack. has be for GC issues see RE 2016-2 issue, I 2016-2 Radwa REFER 5933 f	Smino 9.0 Sim Fix 2 t. ix Pack 5 1 when usin CM, uses r. generatio it easier f ers to obta atication k data by levents to obta the sto obta atication k data by levents to obta and a "foo " NOTE: the en incorree M nonce r in other p FERENCE 10213 for REFERENCE 10212 for are issue, a ENCE: CV or the Citra RENCE: CV	hrough Interim g TLS and andom n, which or remote ain the ey and veraging nce in a orbidden nis CVE ectly used euse roducts; : CVE- the A10 CE: CVE- the and E-2017- ix issue.	01.il ppor wss 9790	om.com/s rt/docviev ?uid=swg2	N.	CLIE	
<b>Cloud Orchestra</b>	tor		01/0							
IBM Cloud Orches using policy-base	strator is a clou	ıd manag	ement p	latform fo	or automa	ting pro	ovisioning	of	cloud s	services
NA	08-02-2017	2.1	IBM Cloud Orchestrator could allow a local authenticated attacker to cause the server to slow down for a short period of time by using a specially crafted and malformed URL. <b>REFERENCE: CVE-2016-</b> 0206			m.co /doo id=s	://www.il om/suppo cview.wss wg2C100	rt ?u	A-IBI CLOU 2802	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	Į	8-9	9-10

Gain Information	08-02-2017	2.1	Vulnerability has been identified in tasks, backend object generated for handling any action performed by the application in IBM Cloud Orchestrator. It is possible for an authenticated user to view any task of the current users domain. <b>REFERENCE: CVE-2016-</b> 0202	http://www.ib m.com/support /docview.wss?u id=swg2C10001 34	A-IBM- CLOUD- 280217/108
Cloud Orchestra				ng provisioning of	cloud comicoc
IBM Cloud Orchestrator is a cloud management platform for automating provisioning of cloud services using policy-based tools; IBM SmartCloud Orchestrator V2.3 is a comprehensive open cloud					
management platform that automates the delivery of cloud services.					
NA	08-02-2017	1.7	A vulnerability has been identified in IBM Cloud Orchestrator services/[action]/launch API. An authenticated domain admin user might modify cross domain resources via a /services/[action]/launch API call, provided it would have been possible for the domain admin user to gain access to a resource identifier of the other domain. <b>REFERENCE: CVE-2015-</b> 7494	http://www.ib m.com/support /docview.wss?u id=swg2C10001 40	A-IBM- CLOUD- 280217/109
Gain Information	08-02-2017	2.1	Vulnerability has been identified in the IBM Cloud Orchestrator task API. The task API might allow an authenticated user to view background information associated with actions performed on virtual machines in projects where the user belongs to. <b>REFERENCE: CVE-2016- 0203</b>	http://www.ib m.com/support /docview.wss?u id=swg2C10001 40	A-IBM- CLOUD- 280217/110
CV Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

Cross Site Scripting	01-02-2017	3.5	IBM Cognos Business Intelligence and IBM Cognos Analytics are vulnerable to stored cro site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerabilit to inject malicious scrip into a Web page which	y 7 y	A-IBM- COGNO- 280217/111
			would be executed in a victim's Web browser within the security cont of the hosting Web site, once the page is viewed An attacker could use th vulnerability to steal th victim's cookie-based authentication credenti <b>REFERENCE: CVE-201</b>	l. his e ials.	
Cognos Business			0217		
IBM Cognos Busir Cross Site Scripting	1ess Intelligenc 01-02-2017	ze is a we	b-based, integrated busin IBM Cognos TM1 is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerabilit using a specially-crafted URL to execute script in victim's Web browser within the security cont of the hosting Web site, once the URL is clicked. attacker could use this vulnerability to steal th victim's cookie-based authentication credenti	e http://www- 01.ibm.com/su pport/docview. wss?uid=swg21 995691 e http://www- ws- second second a http://www- port/docview. wss?uid=swg21 995691 a http://www- alles http://www- second a http://www-	by IBM. A-IBM- COGNO- 280217/112

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

			0218			
<b>Cognos Disclosu</b>	re Managemen	nt 🛛	L			
<b>U</b>	•		a reporting and process au	tomation solutior	n designed to	
_			vtics with narrative analy			
environment.	1		, ,		,	
Execute Code	15-02-2017	6.8	IBM Cognos Disclosure	http://www-	A-IBM-	
			Management 10.2 could	01.ibm.com/su	COGNO-	
			allow a malicious attacker	pport/docview.	280217/113	
			to execute commands as a	wss?uid=swg21	/	
			lower privileged user that	991584		
			opens a malicious	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
			document. IBM Reference			
			#: 1991584.			
			<b>REFERENCE: CVE-2016-</b>			
			6077			
Commerce On Cl	oud: Websnhei	re Comm	erce; Websphere Commerce	Developer		
			inced commerce capabilities		kly and easily	
	•		oss every customer touch po			
			can deliver seamless and con			
	=		eveloper is the developm			
WebSphere Com	• •					
Denial of	01-02-2017	10	IBM WebSphere	http://www.ib	A-IBM-	
Service	01 01 101/		Commerce contains an	m.com/support	COMME-	
			unspecified vulnerability	/docview.wss?u	280217/114	
			that could allow disclosure	id=swg2199275	200217/111	
			of user personal data,	9		
			performing of			
			unauthorized			
			administrative operations,			
			and potentially causing a			
			denial of service.			
			REFERENCE: CVE-2016-			
			6090			
Connections	<u> </u>					
	is a leading bus	siness so	cial network platform that he	lps you get work d	one.	
Cross Site	08-02-2017	3.5	IBM Connections 5.5 and	http://www.ib	A-IBM-	
Scripting			earlier is vulnerable to	m.com/support	CONNE-	
			possible host header	/docview.wss?u	280217/115	
			injection attack that could	id=swg2198833		
			cause navigation to the	8		
			attacker's domain.			
			<b>REFERENCE: CVE-2016-</b>			
			0310			
Cross Site	08-02-2017	3.5	IBM Connections is	http://www.ib	A-IBM-	
Scripting			vulnerable to cross-site	m.com/support CONNE-		
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						

			improj user-si remote exploit using a URL to victim within of the b once th attacke vulner victim auther	ng, caused per valida upplied in e attacker this vuln a specially execute s s Web bro the secur hosting W he URL is er could us ability to s s cookie-h tication c <b>RENCE: CV</b>	tion of put. A could erability -crafted script in a owser ity contex eb site, clicked. A se this steal the pased redentials	id= 0 ct	ocview.wss swg21986		2802	217/116
NA	08-02-2017	4	IBM Co earlier possib attack the dis inappr images	onnections is vulnera le link ma that could play of opriate ba s. <b>RENCE: CV</b>	able to nipulation l result in ackground	m.c n /dc id= 0	p://www.i com/suppc ocview.wss swg21986	rt ?u	A-IB CON 2802	
Gain Information	08-02-2017	4	earlier attacko sensiti readin return	IBM Connections 5.5 and earlier allows remote attackers to obtain sensitive information by reading stack traces in returned responses. <b>REFERENCE: CVE-2016-</b>			p://www.i com/suppc ocview.wss sswg21986	rt ?u	A-IB CON 2802	
<b>Dashboard Appl</b>			vides vi	sualizatio	n and das	hhoard	l services i	n Ia	azz for	Service
Management. Gain Information	02-02-2017	4.3	IBM Ja Manag remote sensiti caused proper certific	IBM Jazz for Service Management could allow a remote attacker to obtain sensitive information, caused by the failure to properly validate the SSL certificate. An attacker could exploit this		a htt; a m.c /dc id= 1	p://www.i com/suppc ocview.wss swg21997	b ort ?u	A-IB DASI	M-
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8-9	9-10

CV 0-	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	8-9	9-10	
Cross Site Scripting	01-02-2017	4.3	5880 IBM Verse is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. REFERENCE: CVE-2016- 6113			m.c s /dc id= b 5	p://www. com/suppo ocview.ws swg21992	ort s?u	rt DOMIN- ?u 280217/122		
Domino; Inotes IBM Domino (fo applications; IBI IBM Notes client Cross Site Scripting	M iNotes (form 01-02-2017	erly IBM I 3.5	IBM iN to cross This vi users to JavaSc UI thus intend potent creder within <b>REFER</b> 5880	otes) offer lotes is vu ss-site scri ulnerabilit co embed a ript code i s altering t ed functio ially leadi atials discl a trusted <b>RENCE: CV</b>	s a full-fe lnerable pting. y allows arbitrary n the We the nality ng to osure session. <b>TE-2016-</b>	atured httj m.c /dc id= b 5	web-base p://www. com/suppo ocview.ws swg21992	ib ort s?u 283	A-IBI DOM 2802	of IBM's M- IN- 17/121	
<b>Dashdb Local</b> dashDB Local is virtual private c NA	0		REFEF 5935 r-suppo IBM da hard-c that cc attacke the Do databa	ng and an rted infras ashDB Loc oded cred ould allow er to gain a cker conta	alytics te structure al uses entials a remote access to ainer or	s. httj m.c /do	gy for use p://www. com/suppo ocview.ws swg21994	ib ort s?u	A-IBN DASH	М-	
			sensiti using i techni		ation middle						

Cross Site Scripting	01-02-2017	4.3	to cros This vu users t JavaSc UI thus intend potent creden within	otes is vu s-site scri ulnerabilit o embed a ript code i s altering ed functio ially leadi tials discl a trusted <b>RENCE: CV</b>	/doc id=s	m.com/support /docview.wss?u id=swg2199283 5			M- IN- 17/123	
Cross Site Scripting	01-02-2017	4.3	to cros This vu users t JavaSc UI thus intend potent creden within <b>REFER</b> 5882	otes is vu s-site scri alnerabilit o embed a ript code i s altering t ed functio ially leadi tials discl a trusted <b>ENCE: CV</b>	pting. y allows arbitrary n the We the nality ng to osure session. <b>TE-2016-</b>	m.co /doc id=s	//www.i m/suppo view.wss wg21992	rt ?u		IN- 17/124
Cross Site Scripting	01-02-2017	4.3	IBM iNotes is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. <b>REFERENCE: CVE-2016-</b>				m.com/support /docview.wss?u id=swg2199283 5			М- IN- 17/125
Cross Site Scripting	01-02-2017	4.3	2939 IBM iNotes is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure			m.co /doc id=s	://www.i m/suppo wiew.wss wg21992	rt ?u	A-IBN DOM 2802	
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8-9	9-10

			within	a trusted	cossion					
				ENCE: CV						
Filenet Workpla	ce Xt		2700							
Workplace XT is the Workplace XT P8.	an optional File			-	-			-	-	
Execute Code	01-02-2017	6.5	could a attacke arbitra allow t execute the vul	leNet Wor Illow a rep ry files, w he attacke e arbitrar nerable so ENCE: CV	d id=sv 8	//www.i m/suppc view.wss wg21994	ort l s?u 2	A-IBM FILEN 28021		
<b>Forms Experience</b> IBM Forms Experience interactive applic	erience Builde	r empov	vers bus	iness us	ers to c	reate c	ompellin	g, m	ulti-c	hannel
NA	01-02-2017	3.5	IBM Fo Builder suscep side red (SSRF) applica interfac some in disclos resource <b>REFER</b> 6001	m.co /doc	//www.i m/suppo view.wss wg21991	ort l s?u 2	A-IBM FORM 28021			
General Parallel IBM Spectrum So file storage or a c as IBM General I capacity with no	cale is a flexible cost optimized l Parallel File Sy	e softwa arge-sca	re-define ale conter	nt reposit	ory; IBM	Spectru	m Scale, j	previo	ously	knowr
Execute Code; Overflow	01-02-2017	9	IBM General Parallel File System is vulnerable to a buffer overflow. A remote authenticated attacker could overflow a buffer and execute arbitrary code on the system with root privileges or cause the server to crash.			m.co /doc id=ss 39	http://www.ib m.com/support /docview.wss?u id=ssg1S10096 39			I- R- L7/129
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	9	9-10

			REFEF 6115	RENCE: CV	Æ-2016-						
Infosphere Data	stage										
IBM InfoSphere I		rates dat	a acros	s multiple	systems	usin	ıg a l	nigh per	forn	nance	parallel
framework, and i											
Gain	01-02-2017	5		foSphere				//www.i		A-IB	M-
Information				nation Serv	ver stores			, n/suppo	INFO	S-	
			sensiti	ve inform	ation in			view.wss			17/130
			URL pa	arameters	. This ma			vg21995			,
			· ·	informati		5		0			
			disclos	sure if una	uthorized	d					
			parties	s have acco	ess to the	Ś					
			-	via server l							
				er header o	0						
			brows	er history.							
			REFEF	RENCE: CV	'E-2016-						
			8982								
Infosphere Data	stage; Infosph	ere Infor	rmation	Server; In	<i>ifospher</i>	e Infe	form	ation Se	rvei	r On C	loud
IBM InfoSphere I											
framework, and	it supports e	xtended	metada	ata manag	gement a	and	ente	rprise d	conn	ectivi	ty; IBM
InfoSphere Infor					0			-			
of products that	enable you to u	nderstar	nd, clean	se, monito	or, transf	orm,	, and	deliver	data	a, as w	ell as to
collaborate to bri	idge the gap bet	ween bu	siness a	nd IT.							
Cross Site	01-02-2017	IBM In	foSphere	e h	http:/	//www.i	b	A-IB	M-		
Scripting			is vulnerable to cross-				m.cor	n/suppo	ort	INFO	S-
			frame	scripting,	caused by	у /	/docv	view.wss	?u	2802	17/131
			insuffi	cient HTM	lL iframe	i	d=sw	vg21995	25		
			protec	tion. A rer	note	7	7				
				er could ex	•	S					
			vulner	ability usi	ng a						
			-	lly-crafted							
			0	te to a we		ie					
				er controls							
				er could us							
				ability to o							
			· ·	cking or o							
				side brow	ser						
			attack								
				RENCE: CV	'E-2016-	•					
			9000								
Cross Site	01-02-2017	3.5		foSphere				//www.i		A-IB	
Scripting				nation Serv				n/suppo		INFO	
				ns a Path-i				view.wss		2802	17/132
				neet impor			_	vg21995	15		
			vulner	ability tha	t allows	5	5				
CV											
Scoring 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8		8-9	9-10
Scale											

			attackers to render a page in quirks mode thereby facilitating an attacker to inject malicious CSS. <b>REFERENCE: CVE-2016-</b> <b>8999</b>		
Denial of Service	01-02-2017	7.5	IBM InfoSphere Information Server is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. <b>REFERENCE: CVE-2016- 6059</b>	http://www.ib m.com/support /docview.wss?u id=swg2199168 3	A-IBM- INFOS- 280217/133
Execute Code; Gain Information	08-02-2017	1.9	IBM InfoSphere Information Server could allow a local user under special circumstances to execute commands during installation processes that could expose sensitive information. <b>REFERENCE: CVE-2015-</b> <b>7493</b>	http://www.ib m.com/support /docview.wss?u id=swg2198203 4	A-IBM- INFOS- 280217/134
Gain Information	01-02-2017	4	IBM InfoSphere Information Server contains a vulnerability that would allow an authenticated user to browse any file on the engine tier, and examine its contents. <b>REFERENCE: CVE-2016-</b> <b>5994</b>	http://www.ib m.com/support /docview.wss?u id=swg2199217 1	A-IBM- INFOS- 280217/135
Cross Site Scripting	01-02-2017	4.3	IBM InfoSphere Information Server is vulnerable to cross-frame scripting, caused by	http://www.ib m.com/support /docview.wss?u id=swg2199168	A-IBM- INFOS- 280217/136
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

			protec attacke vulner special naviga attacke attacke vulner clickja client-	cient HTM tion. A rer er could ex ability usi lly-crafted te to a we er controls er could us ability to o cking or o side brow S. RENCE: CV	note kploit this ng a URL to b page th s. An se this conduct ther ser	e					
Inotes			3704								
IBM iNotes (forn	nerly IBM Lotus	iNotes)	is a web	-based em	ail client	for IB	M No	tes.			
Cross Site Scripting	01-02-2017	4.3	IBM iN to cros This vu users t JavaSc UI thus intend potent creden within <b>REFEF</b> 5881	otes is vu s-site scri ulnerabilit o embed a ript code i s altering ed functio ially leadi itials discl a trusted <b>RENCE: CV</b>	Inerable pting. y allows arbitrary n the We the nality ng to osure session.	b 2	tp://v .com/ locvie	www.i suppo w.wss 21995	ort ?u	A-IBI INOT 2802	
Integration Bus	: Websphere M	essaae B								I	
IBM Integration	· · · · · · · · · · · · · · · · · · ·			(ESB) that	offers a	fast. si	imple	wav fo	or sy	vstem	s and
applications to c											
Bus (ESB) built f				-	-				-		
NA	01-02-2017	-2017 4.3 IBI un con all aut pro cre <b>RE</b>		IBM Integration Bus, under non default configurations, could allow a remote user to authenticate without providing valid credentials. <b>REFERENCE: CVE-2016-</b> <b>8918</b>			.com/ locvie =swg2	www.i suppo w.wss 21995	ort ?u 07		G- 17/138
NA	01-02-2017	2.1	WebSp broker	tegration ohere Mes sets inco ssions for	sage rrect	m. /d	m.com/support				M- G- 17/139
CV 0-1 Scoring Scale	l 1-2	2-3	3-4	4-5	5-6	6-7	7	7-8		8-9	9-10

			that could allow a local attacker to manipulate certain files. <b>REFERENCE: CVE-2016-</b> 0394	3	
NA	15-02-2017	4.3	IBM WebSphere Message Broker 9.0 and 10.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM Reference #: 1997906. <b>REFERENCE: CVE-2016- 9010</b>	http://www.ib m.com/support /docview.wss?u id=swg2199790 6	A-IBM- INTEG- 280217/140
Denial of Service	15-02-2017	8.5	IBM Integration Bus 9.0 and 10.0 and WebSphere Message Broker SOAP FLOWS is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. IBM Reference #: 1997918. <b>REFERENCE: CVE-2016- 9706</b>	http://www.ib m.com/support /docview.wss?u id=swg2199791 8	A-IBM- INTEG- 280217/141

## Jazz Reporting Service

IBM Jazz Reporting Service is an alternative to the complex reporting capabilities that are available in many Rational products and solutions. The Jazz Reporting Service creates reports from the tools in the IBM Rational solution for Collaborative Lifecycle Management (CLM). It is designed for non-technical practitioners who simply want to find information about their software projects and socialize that information in their enterprise through dashboards.

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

CV Scoring Scale	1-2	2-3	3-4	4-5	5-6		6-7	7-8		8-9	9-10	
Cross Site Scripting	01-02-2017	3.5	IBM Jazz Reporting Service (JRS) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web				http://www.ib m.com/support /docview.wss?u id=swg2199115 4			A-IBM-JAZZ - 280217/145		
Cross Site Scripting	01-02-2017	3.5	Service to crost This vu users to JavaScr UI thus intende potenti creden within	zz Report e (JRS) is w s-site scri ilnerabilit o embed a ript code i altering ed functio ially leadi tials discl a trusted ENCE: CV	vulnerabl pting. by allows arbitrary in the We the mality ng to osure session.	/docview.wss?u id=swg2199115 3 eb			ort ?u	t - u 280217/14		
Cross Site Scripting	01-02-2017	3.5	Service to crost This vu users to JavaScr UI thus intende potenti creden within	zz Report e (JRS) is v s-site scri ulnerabilit o embed a ript code i altering ed functio ially leadi tials discl a trusted ENCE: CV	vulnerabl pting. cy allows arbitrary in the We the onality ng to osure session.	eb	m.com /docy	//www.i m/suppo view.wss vg21991	ort ?u	-	M-JAZZ 17/143	
Cross Site Scripting	01-02-2017	3.5	vulnera scriptin vulnera to emb JavaScr UI thus intende potenti creden within	zz Founda able to cro ng. This ability allo ed arbitra ript code i altering ed functio ially leadi tials discl a trusted <b>ENCE: CV</b>	èb	http://www.ib m.com/support /docview.wss?u id=swg2199115 4			A-IBM-JAZZ - 280217/142			

				within	a trusted	session.					
	a LCMS I ess objec	Premier on	goals.	IBM Ke on Clor cross-s vulner to emb JavaSc UI thus intend potent	IBM Kenexa LCMS Premier on Cloud is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.		r http: m.co /doc id=sv 7	http://www.ib m.com/support /docview.wss?u id=swg2199206		A-IBM KENE	-
Gain Informatio	n	)1-02-2017	4	IBM Ja Service remote sensiti caused JSON s sendin an atta this vu sensiti	zz Reporti e (JRS) cou e attacker ve informa l by not res erializatio g a direct cker could lnerability ve informa <b>RENCE: CV</b>	Id allow to obtain ation, stricting n. By request, l exploit to obtain ation.	a m.co /doc id=sv 4	//www.i m/suppo view.wss wg21991	ort ?u	A-IBM - 28021	-JAZZ 7/147
Execute Co Cross Site Scripting	de; 0	01-02-2017	3.5	intend potent creden within <b>REFER</b> 5899 IBM Ja Service to HTM remote inject n code, w would victim	s altering t ed functio ially leadin itials discle a trusted <b>RENCE: CV</b> zz Reporti e (JRS) is v AL injectio e attacker malicious I vhich whe be execute s Web bro the securi hosting sit <b>RENCE: CV</b>	nality ng to osure session. <b>E-2016-</b> ng rulnerable n. A could HTML n viewed ed in the owser ity contex e.	e m.co /doc id=sv 3	//www.i m/suppo view.wss wg21991	ort ?u	A-IBM - 28021	-JAZZ 7/146

Scoring	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	<b>9-1</b> 0
Scale										

			REFERENCE: CVE-2016- 5951		
Cross Site Scripting	01-02-2017	3.5	IBM Kenexa LCMS Premier on Cloud is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. <b>REFERENCE: CVE-2016-</b> <b>5948</b>	http://www.ib m.com/support /docview.wss?u id=swg2199206 7	A-IBM- KENEX- 280217/149
NA	01-02-2017	4	IBM Kenexa LCMS Premier on Cloud stores user credentials in plain in clear text which can be read by an authenticated user. <b>REFERENCE: CVE-2016-</b> <b>5950</b>	http://www.ib m.com/support /docview.wss?u id=swg2199206 7	A-IBM- KENEX- 280217/150
NA	01-02-2017	4	IBM Kenexa LCMS Premier on Cloud could allow an authenticated user to obtain sensitive user data with a specially crafted HTTP request. <b>REFERENCE: CVE-2016-</b> <b>5949</b>	http://www.ib m.com/support /docview.wss?u id=swg2199227 6	A-IBM- KENEX- 280217/151
SQL Injection	01-02-2017	6.5	IBM Kenexa LCMS Premier on Cloud is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back- end database. <b>REFERENCE: CVE-2016-</b> <b>5952</b>	http://www.ib m.com/support /docview.wss?u id=swg2197680 5	A-IBM- KENEX- 280217/152
Cross Site Request	01-02-2017	6.8	IBM Kenexa LCMS Premier on Cloud is vulnerable to	http://www.ib m.com/support	A-IBM- KENEX-
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

Forgery			cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts./docview.wss?u id=swg2199206 7280217/153REFERENCE: CVE-2016- 593771000000000000000000000000000000000000
		-	ganizations to seamlessly integrate both formal and social and performance support strategy.
Gain Information	01-02-2017	2.1	IBM Kenexa LMS on Cloud allows web pages to be stored locally which can be read by another user on 
Cross Site Scripting	01-02-2017	3.5	IBM Kenexa LMS on Cloud is vulnerable to cross-site scripting. Thishttp://www.ib m.com/support 
Directory Traversal	01-02-2017	3.5	IBM Kenexa LMS on Cloud could allow a remote attacker to traverse directories on the system.http://www.ib 
Cross Site	01-02-2017	3.5	IBM Kenexa LMS on Cloud http://www.ib A-IBM-
CV Scoring Scale	l 1-2	2-3	3-4     4-5     5-6     6-7     7-8     8-9     9-10

Scripting			scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. <b>REFERENCE: CVE-2016- 5940</b>				m.com/support /docview.wss?u id=swg2199207 2			KENI 2802	EX- 17/157
Directory Traversal	01-02-2017	4	IBM Ke could a attacke directo An atta special reques sequer arbitra system	allow a rep er to trave ories on th acker coul lly-crafted at containi aces (//) ary files or	mote erse d system d send a l URL ng dot do to view n the	m. /d id: 2	.com locvi	www.i/suppo ew.wss 21992	ort ?u	A-IBI KENI 2802	
SQL Injection	01-02-2017	5.5	is vuln injectio attacko special statem allow t add, m inform end da	enexa LMS erable to on. A remo er could so lly-crafted ents, which he attacko odify or d ation in the tabase. EENCE: CV	SQL ote end I SQL ch could er to view elete he back-	L m.com/support d /docview.wss?u d id=swg2199207 QL 2 could to view, ete back-			ort ?u	A-IBI KENI 2802	
Execute Code	01-02-2017	6.5	IBM Ke could a attacke arbitra allow t execut the vul	M Kenexa LMS on Cloud uld allow a remote cacker to upload bitrary files, which could ow the attacker to ecute arbitrary code on e vulnerable server. EFERENCE: CVE-2016-		m. /d d id= 2	-		ort ?u	A-IBI KENI 2802	
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	ł	8-9	9-10

Execute Code	01-02-2017	6.5	IBM Kenexa LMS on Cloud could allow a remote attacker to upload arbitrary files, which could allow the attacker to execute arbitrary code on the vulnerable server. <b>REFERENCE: CVE-2016-</b> 8931	http://www.ib m.com/support /docview.wss?u id=swg2199207 2	A-IBM- KENEX- 280217/161	
SQL Injection	01-02-2017	6.5	IBM Kenexa LMS on Cloud is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back- end database. <b>REFERENCE: CVE-2016-</b> <b>8930</b>	http://www.ib m.com/support /docview.wss?u id=swg2199207 2	A-IBM- KENEX- 280217/162	
SQL Injection	01-02-2017	6.5	IBM Kenexa LMS on Cloud is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back- end database. <b>REFERENCE: CVE-2016-</b> <b>8928</b>	http://www.ib m.com/support /docview.wss?u id=swg2199207 2	A-IBM- KENEX- 280217/163	
SQL Injection	01-02-2017	6.5	IBM Kenexa LMS on Cloud is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back- end database. <b>REFERENCE: CVE-2016-</b> 5939	http://www.ib m.com/support /docview.wss?u id=swg2199212 9	A-IBM- KENEX- 280217/164	
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Kenexa Lms On (	Cloud									
IBM Kenexa LM			-		-	-	te both f	orm	al and	d social
learning into a co Cross Site Scripting	01-02-2017	3.5	IBM Ke 13.1 an vulner scripti vulner to emb JavaSc UI thus intend potent creder within	enexa LMS and 13.2 - 1 vable to cro ng. This vability allo oed arbitra ript code i s altering t ed functio cially leadi ntials discl a trusted <b>RENCE: CV</b>	5 on Cloud 3.2.4 is ows users ary n the Wel the nality ng to osure session.	http m.co /doo id=s 2				4- 5X- 17/165
Kenexa Lms On (									_	
IBM Kenexa LM learning into a co			0			0	te both f	orm	al and	d social
NA	01-02-2017	3.5	IBM Ke 13.1 an could a attacke clickin victim Web si attacke vulner victim possib attacks <b>REFEF</b> 8911	enexa LMS nd 13.2 - 1 allow a rer er to hijacl g action of . By persus to visit a r ite, a remo er could ex ability to l 's click act ly launch f s against t <b>RENCE: CV</b>	5 on Cloud 3.2.4 note k the f the ading a nalicious ote kploit this hijack the ions and further he victim. <b>TE-2016-</b>	http m.cc /doc id=s 2	://www.i om/suppo cview.wss wg21993	rt ?u		EX- 17/166
Cross Site Scripting	01-02-2017	3.5	13.1 an vulner scripti vulner to emb JavaSc UI thus intend	IBM Kenexa LMS on CloudI13.1 and 13.2 - 13.2.4 isIvulnerable to cross-siteIscripting. ThisI		m.co /doo id=s 2	http://www.ib m.com/support /docview.wss?u id=swg2199398 2		t KENEX- u 280217/16	
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	3	8-9	<b>9-1</b> 0

CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8-9	9-10
Directory Traversal	01-02-2017	4	IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 could allow a remote attacker to traverse directories on the system. An attacker could send a			m.co /do id=s	http://www.ib m.com/support /docview.wss?u id=swg2199398 2		A-IBM- KENEX- 280217/171	
NA	01-02-2017	4	13.1 ar stores sensiti log file by an a	IBM Kenexa LMS on Cloudhttp://www.ib13.1 and 13.2 - 13.2.4m.com/supportstores potentially/docview.wss?usensitive information in inid=swg2199398log files that could be read2by an authenticated user.REFERENCE: CVE-2016-				A-IBN KENI 2802		
Directory Traversal	01-02-2017	4	13.1 ar could a attacked directo An atta special reques dot" se view at system	enexa LMS ad 13.2 - 1 allow a rep er to trave ories on th acker coul ly-crafted t containi quences ( rbitrary fi a.	3.2.4 note erse d send a URL ng "dot [//] to les on the	em. 2 l a t b t b t he				М- ЕХ- 17/169
Cross Site Scripting	01-02-2017	3.5	within REFER 6125 IBM Ke 13.1 ar vulner scripti vulner to emb JavaScr UI thus intend potent creden within	tials discl a trusted ENCE: CV enexa LMS ad 13.2 - 1 able to cro ng. This ability allo ed arbitra ript code i s altering t ed functio ially leadi tials discl a trusted ENCE: CV	session. <b>TE-2016</b> - S on Cloud .3.2.4 is oss-site ows users ary n the Wel the nality ng to osure session.	m.co /do id=s 2	o://www.i om/suppo cview.wss swg21993	ort s?u	A-IBI KENI 2802	

			specially-crafted URL request containing "dot dot" sequences (//) to view arbitrary files on the system. <b>REFERENCE: CVE-2016-</b> <b>6126</b>		
Gain Information	01-02-2017	4	IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 discloses answers to security questions in a response to authenticated users. <b>REFERENCE: CVE-2016-</b> <b>6122</b>	http://www.ib m.com/support /docview.wss?u id=swg2199398 2	A-IBM- KENEX- 280217/172
Execute Code	01-02-2017	6.5	IBM Kenexa LMS on Cloud 13.1 and 13.2 - 13.2.4 could allow a remote attacker to upload arbitrary files, which could allow the attacker to execute arbitrary code on the vulnerable server. <b>REFERENCE: CVE-2016-</b> <b>6124</b>	http://www.ib m.com/support /docview.wss?u id=swg2199398 2	A-IBM- KENEX- 280217/173

Maximo Asset Management; Maximo For Aviation; Maximo For Energy Optimization; Maximo For Government; Maximo For Life Sciences; Maximo For Nuclear Power; Maximo For Oil And Gas; Maximo For Transportation; Maximo For Utilities

IBM Maximo Asset Management is a comprehensive solution for managing physical assets on a common platform in asset-intensive industries. It offers "built in" mobile access, out-of-the box mapping, crew management and analytical insight; IBM Maximo for Aviation creates greater insight into the health of the many components of an airplane; Optimize energy efficiency of assets with IBM Maximo Asset Management for Energy Optimization; IBM Maximo for Government is a system that is compliant with Federal Acquisition Regulation (FAR) requirements; IBM Maximo for Life Sciences is an integrated asset management system for managing tools, equipment, facilities, mobile & IT assets across the enterprise; IBM Maximo for Nuclear Power is an enterprise asset management system that provides a single platform for managing the assets of nuclear plants and fleets; Maximo for Oil and Gas is a complete enterprise asset management solution that helps manage production equipment, facilities, transportation and infrastructure assets on a single, integrated platform; IBM Maximo for Transportation provides enterprise asset management best practices to improve the productivity of all types of transportation assets; IBM Maximo for Utilities offers a complete solution for work and asset management across business units, including gas and electrical transmission, distribution, power generation, water treatment, and wastewater treatment in a single platform and database.

Cross Site Scripting	08-02-2017	4.3	IBM Maximo Asset Management is vulnerable	1 / /	A-IBM-
Scripting			Management is vuinerable	m.com/support	MAAIM-

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

			to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. <b>REFERENCE: CVE-2016-</b> <b>5902</b>	/docview.wss?u id=swg2198825 2	280217/174
Gain Information	01-02-2017	5	IBM Maximo Asset Management could disclose sensitive information from a stack trace after submitting incorrect login onto Cognos browser. <b>REFERENCE: CVE-2016-</b> <b>5896</b>	http://www.ib m.com/support /docview.wss?u id=swg2198785 5	A-IBM- MAXIM- 280217/175

Maximo Asset Management; Maximo For Aviation; Maximo For Life Sciences; Maximo For Nuclear Power;Maximo For Oil And Gas;Maximo For Transportation; Maximo For Utilities; Smartcloud Control Desk; Tivoli Asset Management For It; Tivoli Change And Configuration Management Database; Tivoli Integration Composer; Tivoli Service Request Manager

IBM Maximo Asset Management is a comprehensive solution for managing physical assets on a common platform in asset-intensive industries. It offers "built in" mobile access, out-of-the box mapping, crew management and analytical insight; IBM Maximo for Aviation creates greater insight into the health of the many components of an airplane; Optimize energy efficiency of assets with IBM Maximo Asset Management for Energy Optimization; IBM Maximo for Government is a system that is compliant with Federal Acquisition Regulation (FAR) requirements; IBM Maximo for Life Sciences is an integrated asset management system for managing tools, equipment, facilities, mobile & IT assets across the enterprise; IBM Maximo for Nuclear Power is an enterprise asset management system that provides a single platform for managing the assets of nuclear plants and fleets; Maximo for Oil and Gas is a complete enterprise asset management solution that helps manage production equipment, facilities, transportation and infrastructure assets on a single, integrated platform; IBM Maximo for Transportation provides enterprise asset management best practices to improve the productivity of all types of transportation assets; IBM Maximo for Utilities offers a complete solution for work and asset management across business units, including gas and electrical transmission, distribution, power generation, water treatment, and wastewater treatment in a single platform and database.

0 ,	,		01		
Cross Site	01-02-2017	3.5	IBM Maximo Asset	http://www.ib	A-IBM-
Scripting			Management is vulnerable	m.com/support	MAXIM-
			to cross-site scripting.	/docview.wss?u	280217/176
			This vulnerability allows	id=swg2199189	
			users to embed arbitrary	3	
			JavaScript code in the Web		

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

			meena							
Cross Site Scripting	08-02-2017	3.5	IBM Rational Team Concert 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality		m.co /doc id=s 4	://www.i m/suppo wiew.wss wg21997	rt ?u	A-IBM RATIO 2802		
Cross Site Scripting	01-02-2017	3.5	vulner scripti vulner to emb JavaScr UI thus intend potent creden within <b>REFER</b> 6030	6061 IBM Jazz Foundation is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. REFERENCE: CVE-2016-		m.co /doc id=s 7 b	s://www. om/suppo view.wss wg21996	ort ?u 09		)- 17/178
<b>Rational Collabo</b> The Rational solu tools that work to Cross Site Scripting	ution for Colla	oorative l	intend potent creden within <b>REFER</b> <b>6072</b> <i>ement</i> Lifecycle IBM Ja vulner scripti vulner to emb JavaSc UI thus intend potent creden within <b>REFER</b>	s altering ted function ially leadination is a trusted sence: cv Managen zz Foundation is a trusted sence is a trusted sence is a sence is a sence is a sence is a trusted sence is a trusted sence is a trusted sence cv a trusted sence is a tr	onality ng to osure session. / <b>E-2016-</b> nent (CLM ation is oss-site ows users ary in the We the onality ng to osure session.	http: m.co /doc id=s 7	et of sean s://www. m/suppo cview.wss wg21996	.ib ort ?u	A-IBM RATIO	1-

			creden within	ially leadi tials discl a trusted ENCE: CV	osure session.						
Cross Site Scripting	15-02-2017	3.5	vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1998515. <b>REFERENCE: CVE-2016- 8968</b>				m.cor /docv	//www. n/supp riew.ws rg21998	ort s?u	A-IBM RATIO 2802	
NA	01-02-2017	4	produc attacke item ti have p	IBM Jazz technology based products might allow an attacker to view work item titles that they do not have privilege to view. <b>REFERENCE: CVE-2016-</b>				r//www n/supp riew.ws vg21996	ort s?u	A-IBM RATIO 2802	
Gain Information	08-02-2017	4	An uns vulner Team S some c inform authen	pecified ability in I Server ma leploymer ation to a ticated us E <b>ENCE: CV</b>	y disclose nt n er.	e /	m.cor /docv	//www. n/supp riew.ws vg21997	ort s?u	A-IBM RATIO 2802	
NA	01-02-2017	6	IBM Jazz Foundation could allow an authenticated user to take over a previously logged in user due to session expiration not being enforced. <b>REFERENCE: CVE-2016-</b> 6040			r i 7	m.cor /docv	r//www n/supp riew.ws 7g21996	ort s?u	A-IBM RATIO 2802	
Rational Doors Manager;Ration							-			ality	
CV											

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

## Manager;Rational Team Concert

IBM Rational DOORS Next Generation is a requirements management tool that provides a smarter way to define, trace, analyze, and manage requirements; IBM Rational Engineering Lifecycle Manager visualizes, analyzes and organizes engineering lifecycle data and data relationships; Rational Quality Manager is a test management tool. It stores test cases, records test execution and results, m aps testing onto requirements and tracks defects; IBM Rational Rhapsody Design Manager is collaborative design management software that helps design teams and their stakeholders to share, trace, review and manage designs. Supporting the systems engineering and embedded software development lifecycle, Rational Rhapsody Design Manager helps to effectively manage complexity, reduce risk and improve systems engineering and software quality, design and delivery; IBM Rational Software Architect Design Manager is a collaborative software development and design platform built on Jazz technology; Rational Team Concert is a software development team collaboration tool developed by the Rational Software brand of IBM, who first released it in 2008.

the National Solt		-			2000.					1	
Gain Information	01-02-2017	4	vulner	disclosed ability in ( ations may		n	n.con	//www n/suppo iew.wss	ort	A-IBI RATI 2802	
				administra		'		g21996		2002	17/104
				vment para		7		g21770	0)		
				shown to a		ĺ,					
			attack								
				RENCE: CV	E-2016-						
			2987								
<b>Rational Doors</b> N	Vext Generati	on; Ratio	nal Requ	uirements	Compos	er				•	
IBM Rational DO	ORS Next Gene	eration is	a requir	ements ma	anagemei	nt too	ol tha	t provid	les a	a smar	ter way
to define, trace,	analyze, and r	manage r	equirem	ents; IBM	Rational	Requ	uiren	nents Co	omp	oser s	oftware
empowers teams	to define, mar	nage and	report of	n requiren	nents in a	lifec	cycle	develop	me	nt proj	ject.
Cross Site	08-02-2017	3.5		ational DO			• •	/www.i		A-IBI	
Scripting				ation 4.0, 5	•			n/suppo		RATI	
				vulnerable		'		iew.wss		2802	17/185
				ripting. Th				g21996	64		
				ability allo		5 5	)				
				oed arbitra	5	,					
				ript code i		b					
				s altering t ed functio							
				ially leadi	•						
			-	itials discl	0						
				a trusted							
				RENCE: CV							
			1128		-						
Cross Site	08-02-2017	3.5	IBM Ra	ational DO	ORS Next	t h	ttp:/	/www.i	b	A-IBI	M-
Scripting			Genera	ation 4.0, 5	5.0 and 6.			, n/suppo		RATI	0-
				erable to o	cross-site	e //	docv	iew.wss	?u	2802	17/186
			scripting. This					g21996	64		
			vulner	ability allo	ows users	5 5					
OV											
CV	1.0	2.2	2.4	4 -	FC	C		7.0		0 0	0.10

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

IBM Security Ac	0	4.3	IBM Security Access Manager for Web stores sensitive information in URL parameters. This may	http://www.ib m.com/support /docview.wss?u id=swg2199543	e enterprise. A-IBM- SECUR- 280217/189
Socurity Accoss		integrate	ss Manager For Mobile; Secu d appliance is designed to a ederation to apps running ins	manage Access in	the world of
Information			vulnerability in IBM Rational DOORS Next Generation 4.0, 5.0, and 6.0 could allow a JazzGuest user to see project names. IBM Reference #: 1995547. <b>REFERENCE: CVE-2016-</b> 6060	m.com/support /docview.wss?u id=swg2199554 7	RATIO- 280217/188
Gain Information Gain	08-02-2017	4	intended functionality potentially leading to credentials disclosure within a trusted session. <b>REFERENCE: CVE-2017-</b> <b>1127</b> IBM Rational DOORS Next Generation 5.0 and 6.0 discloses sensitive information in error response messages that could be used for further attacks against the system. <b>REFERENCE: CVE-2016-</b> <b>9748</b> An undisclosed	http://www.ib m.com/support /docview.wss?u id=swg2199146 1 http://www.ib	A-IBM- RATIO- 280217/187 A-IBM-

CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Gain Information	01-02-2017	5		ppScan So some sens		-	//www.ib m/suppor		-IBM- ECUR-
role in software s	IBM Security AppScan Source delivers m role in software security.			IBM AppScan Source uses a one-way hash without salt to encrypt highly sensitive information, which could allow a local attacker to decrypt information more easily. <b>REFERENCE: CVE-2016- 3034</b>			//www.ib m/suppor view.wss? wg219959	A Tt S Uu 23	-IBM- ECUR- 80217/192
Security Appscar IBM Security App and costly data b Execute Code; Overflow	oScan Standar reaches by au 01-02-2017	tomating 9.3	rganizati applicati IBM Aj Edition remote arbitra system improj objects persua open s conten exploit to exec on the contex <b>REFEF</b> 6042	on securit opScan En a could all e attacker ary code on a caused b per handli s in memo ading a vic pecially-cu at, an attac t this vulne cute arbitr system in t as the vi <b>RENCE: CV</b>	y vulnera terprise ow a to execut n the by ng of ry. By tim to rafted eker could erability rary code the same ctim. <b>TE-2016-</b>	bility tes http: m.co e /doc id=sv 8	sting. //www.ib m/suppor view.wss? wg219951	A tt S u 2 1	-IBM- ECUR- 80217/191
			scripti vulner to emb JavaSc UI thus intend potent creder within	able to cro ng. This ability allo bed arbitra ript code i s altering t ed functio ially leadi atials discl a trusted <b>RENCE: CV</b>	ows users ary n the Wel the nality ng to osure session.	id=sv 7	view.wss? wg219953		80217/190

			information through the browsing of testlinks on the server. <b>REFERENCE: CVE-2016-</b> <b>3035</b>			id= 5	ocview.wss swg21987		2802	17/193
Security Director	ry Server;Tivol	i Directo	ory Serv	er						
IBM Security Dire	ectory Server is	s an ente	rprise d	irectory fo	or corpor	ate intr	anets and	the	Interr	net; IBM
Security Director	y Server, forme	erly knov	vn as IBl	M Director	y Server	and IB	M Tivoli D	irec	tory S	erver, is
an IBM implemen	ntation of the Li	ghtweig	ht Direct	ory Acces	s Protoco	ol.				
Execute Code	08-02-2017	2.1	IBM Security Directory Server could allow an authenticated user to execute commands into the web administration tool that would cause the tool to crash. <b>REFERENCE: CVE-2015-</b> <b>1976</b>			m.c /dc id= 5	o://www.i om/suppo ocview.wss swg21980	ort s?u	A-IBI SECU 2802	
Security Guardiu	im									
IBM Security Gua	rdium product	s help to	o ensure	the secur	rity, priva	acy and	l integrity	of in	nform	ation in
your data center.	·	•								
Execute Code	01-02-2017	7.2	Databa applia: local u comma execut <b>REFEF</b> 6065	IBM Security Guardium Database Activity Monitor appliance could allow a local user to inject commands that would be executed as root. <b>REFERENCE: CVE-2016-</b>			p://www.i om/suppo ocview.wss swg21995	ort s?u	A-IB SECU 2802	
<i>Security Identity</i> NA	Manager Virt	ual Appl	liance							
NA	01-02-2017	2.1	Manag stores plain i can be	ecurity Ide er Virtual user crede n clear tex read by a <b>RENCE: CV</b>	Appliance entials in t which local use	e m.d /do id=	http://www.ib m.com/support /docview.wss?u id=swg2199676 1			M- JR- 17/196
Gain Information	01-02-2017	2.1	IBM Security Identity Manager Virtual Appliance does not invalidate session tokens which could allow an unauthorized user with physical access to the			e m.d /do	http://www.ib m.com/support /docview.wss?u id=swg2199676 1			M- JR- 17/197
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	8-9	9-10

CV Scoring 0-1	1-2	2-3	REFERENCE: CVE-2016-       3-4     4-5     5-6	6-7 7-8	8-9 9-10
Gain Information	01-02-2017	5	IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 can be deployed with active debugging code that can disclose sensitive information.	http://www.ib m.com/support /docview.wss?u id=swg2199798 3	A-IBM- SECUR- 280217/200
costs of encrypti	on key manage ment for IBM	ement. It and nor	nent process to help minim offers secure and robust ke IBM storage solutions usin IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. <b>REFERENCE: CVE-2016- 6116</b>	ey storage, key se	rving and key
Cross Site Scripting Security Key Life			IBM Security Identity Manager Virtual Appliance is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. <b>REFERENCE: CVE-2016-</b> <b>9704</b>	http://www.ib m.com/support /docview.wss?u id=swg2199676 1	A-IBM- SECUR- 280217/198
			work station to obtain sensitive information. <b>REFERENCE: CVE-2016-</b> <b>9703</b>		

			6117				
Gain Information	02-02-2017	5	IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. <b>REFERENCE: CVE-2016-</b> <b>6099</b>	http://www.ib m.com/support /docview.wss?u id=swg2199792 4	A-IBM- SECUR- 280217/201		
NA	02-02-2017	5	IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. <b>REFERENCE: CVE-2016-</b> <b>6095</b>	http://www.ib m.com/support /docview.wss?u id=swg2199780 2	A-IBM- SECUR- 280217/202		
NA	01-02-2017	6.4	IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 do not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. <b>REFERENCE: CVE-2016-</b> 6105	http://www.ib m.com/support /docview.wss?u id=swg2199774 1	A-IBM- SECUR- 280217/203		
Execute Code	07-02-2017	6.5	IBM Tivoli Key Lifecycle Manager 2.5, and 2.6 could allow a remote attacker to upload arbitrary files, caused by the improper validation of file extensions, which could allow the attacker to execute arbitrary code on the vulnerable system. <b>REFERENCE: CVE-2016-</b> <b>6104</b>	http://www.ib m.com/support /docview.wss?u id=swg2199798 8	A-IBM- SECUR- 280217/204		
Cross Site Request Forgery	02-02-2017	6.8	IBM Tivoli Key Lifecycle Manager 2.5 and 2.6 is vulnerable to cross-site	http://www.ib m.com/support /docview.wss?u	A-IBM- SECUR- 280217/205		
CV 0-1 Scoring Scale	1 1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10		

							wg21997	794				
Security Key Lifecycle Manager; Tivoli Key Lifecycle ManagerIBM Security Key Lifecycle Manager, formerly Tivoli Key Lifecycle Manager, centralizes, simplifies and automates the encryption key management process to help minimize risk and reduce operational costs of encryption key management. It offers secure and robust key storage, key serving and key lifecycle management for IBM and non-IBM storage solutions using the OASIS Key Management Interoperability Protocol (KMIP).Gain07-02-20172.1IBM Tivoli Key Lifecyclehttp://www.ibA-IBM-												
Gain Information	07-02-2017	2.1	Manag allows stored be rea the sys	er 2.0.1, 2 web page locally wl d by anoth	.5, and 2. es to be nich can ner user c	6 m.co /do id=s on 6	://www.i om/suppc cview.wss wg21997	ort s?u	SECU			
Gain Information	07-02-2017	2.1	Manag stores plain i can be	voli Key L ger 2.0.1, 2 user cred n clear tex read by a <b>RENCE: CV</b>	6 m.co /do id=s r. 3	http://www.ib m.com/support /docview.wss?u id=swg2199795 3			M- R- 17/207			
Gain Information	07-02-2017	4	IBM Ti Manag genera messa sensiti about users,	voli Key L ger 2.0.1, 2 ates an err ge that ind ve inform its environ or associa <b>RENCE: CV</b>	.5, and 2. or cludes ation nment, ted data.	6 m.co /do/ id=s 7	http://www.ib m.com/support /docview.wss?u id=swg2199798 7			M-  R- 17/208		
Cross Site Scripting	07-02-2017	4.3	Manag is vuln scripti vulner to emb	IBM Tivoli Key Lifecycle Manager 2.0.1, 2.5, and 2.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web			http://www.ib m.com/support /docview.wss?u id=swg2199798 4			t SECUR- u 280217/209		
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	3-9	9-10		

			UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. <b>REFERENCE: CVE-2016-</b> <b>6096</b>								
			6096								
Security Privileg	· · · · · · · · · · · · · · · · · · ·	<u> </u>									
IBM Security Pri						nd a	udit	s the ı	use	of pr	ivileged
identities to help									1		
Gain Information	01-02-2017	4	Identity Applian sensitiv generat that wo an auth	ce could e inform ed error uld be av enticatec	r Virtual disclose ation in messages vailable to	m /0 ic s 4	n.con docv d=sw	//www.i n/suppo iew.wss rg21996	ort s?u	A-IBI SECU 2802	
Gain Information	01-02-2017	4.3	IBM Security Privileged Identity Manager Virtual Appliance could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. <b>REFERENCE: CVE-2016-</b>				http://www.ib m.com/support /docview.wss?u id=swg2199661 4			SECUR- 280217/211 A-IBM-	
NA	01-02-2017	5	5966 IBM Security Privileged Identity Manager Virtual Appliance version 2.0.2 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. REFERENCE: CVE-2016- 5964			m /c ic 5	http://www.ib m.com/support /docview.wss?u id=swg2199406 5			A-IBM- SECUR- 280217/212	
Gain	01-02-2017	5		urity Pri	vileged	h	ttp:/	/www.i	ib	A-IBI	M-
CV 0-1	1-2	2-3	3-4	4-5	5-6	6-		7-8		8-9	9-10
Scale											

Information				y Manage a remote a			m/suppo view.wss		ECUR- 30217/213
			obtain	sensitive		id=sv	wg21996		502177215
				ation, cau to set the	-	e 4			
				r the sessi		2			
			-	mode. By					
				epting its					
				hission wit session, ar					
				exploit this					
			vulner	ability to o	capture				
				okie and o					
				ve inform <b>RENCE: CV</b>					
			5958		L 2010				
NA	01-02-2017	6.5		ecurity Pri	0	-	//www.i		-IBM-
				y Manage			m/suppo		ECUR-
				nce allows nticated us		,	view.wss wg21996		30217/214
				l malicious				01	
				be automa					
				ed by the RENCE: CV					
			5990	CENCE: UV	E-2010-				
Social Rendering	g Templates F	or Digita		onnector					
The IBM Social									
content libraries, integrate social d						at use th	e provide	ed web	content to
Cross Site	01-02-2017	4.3		ocial Rend		http:	//www.i	h A-	-IBM-
Scripting		10		ates for Di	0	-	m/suppo		DCIA-
				ctor is vul		· / · · ·	view.wss		30217/215
				site scripti	0		wg21993	89	
				ability allo oed arbitra		5			
				ript code i	-	b			
			UI thu	s altering t	the				
				ed functio					
				ially leadi itials discl					
				a trusted					
				RENCE: CV	'E-2016-				
Constant Constant		n n n Drug d	8936	C t					
Spectrum Contro IBM Spectrum (		<b>U</b>			nat can	significa	ntly imp	rove n	nonitoring,
CV			0.4				<b>7</b> 0		0.10
Scoring 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

automation and Productivity Cent								M	Гivoli	Storage
Cross Site Scripting	01-02-2017	3.5	IBM Tivoli Storage Productivity Center is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. <b>REFERENCE: CVE-2016- 8943</b> IBM Tivoli Storage				p://www.i om/suppo ocview.wss swg21995	ort s?u	A-IBI SPEC 2802	
NA	01-02-2017	3.5					http://www.ib m.com/support /docview.wss?u id=swg2199512 8			M- T- 17/217
Cross Site Request Forgery	01-02-2017	6.8	IBM Ti Product vulner reques could a execut unauth transm that th	voli Stora ctivity Cen able to cro t forgery allow an a e maliciou norized ac nitted from e website <b>RENCE: CV</b>	m.c /dc id= 8	p://www.i om/suppo ocview.wss swg21995	ort s?u	A-IBI SPEC 2802		
Sterling B2b Inter IBM Sterling B2E	Integrator en	ables th	e securi	ty-rich in	tegration	of co	mplex B2	Вр	rocess	es with
diverse partner c Gain Information	08-02-2017	5	IBM Sterling B2B Integrator Standard Edition could allow a remote attacker to obtain sensitive information. By allowing HTTP OPTIONS				http://www.ib m.com/support /docview.wss?u id=swg2198154 9			M- L- 17/219
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8-9	9-10

Gain Information	01-02-2017	5.8	could s crafted vulner to caus disclos inform respor <b>REFEF</b> 0210 IBM St Integra Edition remote conduc	erling B21 ator Stand 1 could all e attacker ct phishin	cially- a er running ver to re he HTTP / <b>E-2016-</b> B lard ow a to g attacks,	g httj m.c /dc id=		-			
			attack. victim crafted attacke vulner URL di a user site that be trus allow t obtain inform further victim. <b>REFEF</b> 6020	an open re By persu to visit a s l Web site er could es ability to splayed to to a malic at would a sted. This the attacks highly sen ation or c r attacks a	e s e						
<i>Sterling Selling A</i> NA	And Fulfillmen	t Found	ation								
Gain Information	01-02-2017	4.3	Manag session the UR unable view d allowe websit error p session	erling Ord ement tra i dentifie L. When a to view a ue to not d permiss re respond bage wher n identifie ed as Base	ne m.c /dc id= 1	http://www.ib m.com/support /docview.wss?u id=swg2199452 1			A-IBM- STERL- 280217/221		
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8-9	9-10	

			URL. REFERENCE: CVE-2016- 5953		
System Storage	Ts3100-ts3200	Tape Li	brary		
			3200 Tape Libraries are wel	ll-suited for handlin	ng the backup,
restore, and arch	ive data-storage	e needs f	or small-to-medium environ	ments.	
NA	08-02-2017	7.5	IBM System Storage TS3100-TS3200 Tape Library could allow an unauthenticated user with access to the company network, to change a user's password and gain remote access to the system. <b>REFERENCE: CVE-2016-</b> 9005	http://www.ib m.com/support /docview.wss?u id=ssg1S10096 56	A-IBM- SYSTE- 280217/222
			Network Capture Add-on		
		ence on	Cloud delivers IBM Tealea	af core capabilities	s in an IBM
managed cloud en				Τ-	
Gain	08-02-2017	4.3	IBM Tealeaf Customer	http://www.ib	A-IBM-
Information			Experience on Cloud Network Capture Add-On could allow a remote attacker to obtain sensitive information, caused by the failure to properly validate the TLS certificate. An attacker	m.com/support /docview.wss?u id=swg2199453 4	TEALE- 280217/223
			could exploit this vulnerability to obtain sensitive information using man in the middle		
			techniques. REFERENCE: CVE-2016- 5900		
Tivoli Storage El	ashcony Mana	aer For	T 5900 Vmware; Tivoli Storage Mai	nager For Virtual I	Invironments
Data Protection	· · · · · · · · · · · · · · · · · · ·	yer ror	mwure, mvon stor uge Mur		
		orage M	anager) is a data protection	nlatform that gives	enternrises a
-		-	n for backup and recovery.	plation in that gives	enter prises a
Cross Site	15-02-2017	6.8	IBM Tivoli Storage	http://www.ib	A-IBM-
Request	15-02-2017	0.0	Manager for Virtual	m.com/support	TIVOL-
Forgery			Environments 7.1	/docview.wss?u	280217/224
			(VMware) is vulnerable to	id=swg2199554	
			cross-site request forgery	5	
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

			which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM Reference #: 1995545. <b>REFERENCE: CVE-2016-</b> 6033								
<b>Tivoli Storage M</b> IBM Spectrum P	rotect (Tivoli St					n p	latfor	m that g	ives	enter	prises a
single point of control and administration for backup and recovery.											
Gain Information	01-02-2017	1.9	Manag may be text via output tracing	voli Stora; er (TSM) e displaye a applicat: while app ; is enable ENCE: CV	password d in plain ion trace plication ed.	l	01.ib ppor	//www- m.com/s t/docvie uid=swg 14	su w.	A-IBI TIVO 2802	
Cross Site Scripting	01-02-2017	3.5	IBM Ti Manag Center cross-s vulner to emb JavaSc UI thus intend potent creden within	0371 IBM Tivoli Storage Manager Operations Center is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. REFERENCE: CVE-2016-			http://www.ib m.com/support /docview.wss?u id=swg2199575 4			A-IB] TIVO 2802	
NA	01-02-2017	4				http://www.ib m.com/support /docview.wss?u id=swg2199575 4			A-IBM- TIVOL- 280217/227		
CV 0- Scoring Scale	1 1-2	2-3	3-4	4-5	5-6		6-7	7-8		8-9	9-10

NA	01-02-2017	4.4	Tivoli Storage Manager Operations Center could allow a local user to take over a previously logged in user due to session expiration not being enforced. <b>REFERENCE: CVE-2016-</b> <b>6043</b> IBM Tivoli Storage				http://www.ib m.com/support /docview.wss?u id=swg2199575 4			A-IBM- TIVOL- 280217/228		
Cross Site Request Forgery	01-02-2017	6.8	Manager Operationsm.com/supportCenter is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.m.com/support /docview.wss?u id=swg2199575REFERENCE: CVE-2016- 60456045					A-IBI TIVO 2802				
Execute Code; Overflow	01-02-2017	7.2	Manag Protect vulner overflo Based A local overflo execut the system	6045The IBM Tivoli StorageManager (IBM SpectrumProtect) AIX client isvulnerable to a bufferoverflow when Journal-Based Backup is enabled.A local attacker couldoverflow a buffer andexecute arbitrary code onthe system or cause asystem crash.REFERENCE: CVE-2016-				http://www.ib m.com/support /docview.wss?u id=swg2199369 5			M- L- 17/230	
Tivoli Storage M	anaaer Fastba	ick	3703									
IBM Spectrum Workstations) is	Protect for V	Vorkstat		-			-	-				
and laptop comp	1											
Execute Code	08-02-2017	6.9	Manag installe remote arbitra system	IBM Tivoli Storage Manager FastBack installer could allow a remote attacker to execute arbitrary code on the system. By placing a specially-crafted DLL in			http://www.ib m.com/support /docview.wss?u id=swg2198890 8			t TIVOL- u 280217/231		
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8		8-9	9-10	

	1									
				tim's path						
			attack	er could ex	xploit this	5				
			vulner	ability wh	en the					
			install	er is execu	ited to ru	n				
			arbitra	ry code o	n the					
				n with priv						
			the vic	-	U					
			REFEF	RENCE: CV	'E-2016-					
			5934							
Tivoli Storage M	anaaer For Sn	ace Man		t					I	
Use Tivoli Storag					move i	nactive	or selde	om-	used	files to
server storage, fr	-	-	-				or bora		ubeu	11100 00
Gain	08-02-2017	1.9		voli Stora	σe	httr	)://www.i	h	A-IBI	M-
Information	00 02 2017	1.7		er HSM fo	0		om/suppc		TIVO	
mormation			Ŭ Ŭ	ws display			cview.wss			17/232
				ted Tivoli	•	,	swg21988		2002	11/252
			51	er passwo	0	8	51121700	12		
			-	ation trace		-				
				ssword ac	-	1				
			-							
			_	is prompt						
			•	ord is chai	0					
				RENCE: CV	E-2016-					
m: 1: 0: 14			5918				7			
Tivoli Storage M								•	C	
IBM Tivoli Stora					eferrea t	o as Da	ta Proteci	tion	for v	Mwarej
provides a comp						1.44	. / /	1.		N/
Gain	01-02-2017	4		voli Stora	0		)://www.i		A-IBI	
Information			_	er for Virt			om/suppo		TIVO	
				nments (\	-		cview.wss		2802	17/233
				lisclose th			swg21995	54		
				ws domai		4				
				itials to a ı						
			<u> </u>	level of pr	0					
				RENCE: CV	'E-2016-					
			6034							
Tivoli Storage M	lanager; Tivol	i Storag	e Mana	ger For V	'irtual Ei	nvironn	nents Dat	a P	rotect	tion For
Vmware										
IBM Spectrum Pr						n platfo	rm that g	ives	enter	prises a
single point of co						-			-	
NA	01-02-2017	2.1		voli Stora	0	-	)://www.i		A-IBI	
				er undiscl			om/suppc		TIVO	
				rypted log			cview.wss		2802	17/234
				itials to Vr		id=	wg21996	19		
			vCente	er that cou	ld be	8				
			obtain	ed by a loo	cal user.					
CV										
CV 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8-9	9-10
Scoring Scale										
Julie										

			REFEF 6110	RENCE: CV	Æ-2016-					
<i>Tririga Applicat</i> IBM TRIRIGA Aj components.		form pr	ovides a	single w	eb-based	set of	design-ti	ime	and	runtime
Cross Site Scripting	01-02-2017	3.5	Platfor cross-s vulner to emb JavaSc UI thus intend potent creden within	RIRIGA Ap m is vulne site scripti ability allo ed arbitra ript code i s altering t ed functio ially leadi itials discl a trusted RENCE: CV	m.co /doc id=s 2	://www.i om/suppo :view.wss wg21991	ort ?u	A-IBM TRIR 2802		
Cross Site Scripting	01-02-2017	4.3	Platfor cross-s vulner to emb JavaSc UI thus intend potent creden within	RIRIGA Ap rm is vulne site scripti ability alle oed arbitra ript code i s altering t ed functio ially leadi itials discl a trusted <b>RENCE: CV</b>	erable to ng. This ows users ory n the Wel the nality ng to osure session.	m.co /doc id=s 5	://www.i om/suppo cview.wss wg21991	ort ?u	A-IBM TRIR 2802	
Urbancode Deplo IBM UrbanCode I Execute Code; Gain		for auto 2.1	IBM Un creates	rbanCode s tempora	Deploy ry files	http m.co	://www.i m/suppo	b ort	A-IBN URBA	/I- AN-
Information			could o inform passwo read by	creates temporary files during step execution that could contain sensitive information including passwords that could be read by a local user. <b>REFERENCE: CVE-2016-</b> 2941			view.wss wg2C100		2802	17/237
NA	01-02-2017	4	could a	IBM UrbanCode Deploy could allow an authenticated user to			http://www.ib m.com/support /docview.wss?u		ort URBAN-	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	3-9	9-10

			multip not pro users e This co behavi trigger	Ucd obje le REST en operly aut editing UC ould affect or of legit ed proces <b>ENCE: CV</b>	ndpoints horizing D objects the imately ses.	22	wg2C100	02		
NA	01-02-2017	5	could a user to Relay A JMX in plugins	banCode illow a ma access th ActiveMQ terface an s on the ag ENCE: CV	llicious e Agent Broker d run gent.	m.co /doo	://www.i om/suppo cview.wss wg2C100	rt ?u	A-IBI URBA 2802	
Gain Information	01-02-2017	5	could a authen access endpoi and CL secure	banCode Illow an ticated us to the RES nts to acc I getReso d role pro ENCE: CV	ser with ST ess API urce perties.	m.co /doo	://www.i om/suppo cview.wss wg2C100	rt ?u	A-IBI URB/ 2802	
NA	01-02-2017	6	could a authen with sp to craft server cause p a remo machin	banCode illow an ticated at becial peri t a script o in a way t processes te UCD ag ne. <b>ENCE: CV</b>	tacker missions on the hat will to run on gent	m.co /doo id=s 18	://www.i om/suppo cview.wss wg2C100	rt ?u	A-IBI URB/ 2802	
Execute Code	01-02-2017	10	IBM Un could a execut special upload code o code o	IBM UrbanCode Deploy could allow a user to execute code using a specially crafted file upload that would replace code on the server. This code could be executed on the UCD agent machines		m.co /doo id=s e 37	://www.i om/suppo cview.wss wg2C100	rt ?u	A-IBI URBA 2802	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	8-9	9-10

			that host customer's production applications. <b>REFERENCE: CVE-2016-</b> 8938
WebSphere App WebSphere App web application	plication Serv		) is a software product that performs the role of a
Cross Site Scripting	01-02-2017	3.5	IBM WebSpherehttp://www.ibA-IBM-Application Server ism.com/supportWEBSP-vulnerable to cross-site/docview.wss?u280217/243scripting. Thisid=swg2199599280217/243vulnerability allows users55to embed arbitrary54JavaScript code in the WebUI thus altering the4intended functionalitypotentially leading to4credentials disclosurewithin a trusted session.8934
Cross Site Scripting	13-02-2017	3.5	IBM WebSpherehttp://www.ibA-IBM-Application Server 7.0, 8.0, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.http://www.ib m.com/support /docview.wss?u id=swg2199774A-IBM- WEBSP- 280217/244IBM Reference #: 1997743 REFERENCE: CVE-2017- 1121http://www.ib m.com/support /docview.wss?u id=swg2199774A-IBM- WEBSP- 
Denial of Service	01-02-2017	7.8	IBM WebSpherehttp://www.ibA-IBM-Application Server may bem.com/supportWEBSP-vulnerable to a denial of/docview.wss?u280217/245service, caused byid=swg2199379280217/245allowing serialized objects77from untrusted sources to77run and cause the66consumption of resources.8REFERENCE: CVE-2016-6
CV 0-1 Scoring Scale	l 1-2	2-3	3-4     4-5     5-6     6-7     7-8     8-9     9-10

			8919						
Websphere Extr	eme Scale		•			<b>I</b>		<b>I</b>	
WebSphere App		er (WAS)	is a	software	product	that 1	performs	the r	ole of a
web application					•	-			
Gain	08-02-2017	2.1	IBM W	ebSphere	eXtreme	http:	://www.i	b A-I	BM-
Information				ind the We			m/suppo		BSP-
mormation				ower XC10	-		view.wss		)217/246
				nce allow			wg21971		217/210
				ve data to			wg21)/1	05	
				ry instead	-	/			
				ritten whi	-				
				a local use					
				istrator pr	ivneges t	.0			
				sensitive					
			inform						
				RENCE: CV	E-2015-				
			7418						
Websphere Mess									
IBM Integratio		rmerly		as Web	<b>.</b>	Messa	0	ker) i	
integration broke	er from the We	ebSphere	product	t family t	hat allow	ws busi	ness info	ormation	to flow
between disparat	te applications	across m	ultiple h	ardware a	and softw	are plati	forms.		
Gain	01-02-2017	5	The W	ebAdmin o	context	http:	://www.i	b A-I	BM-
Information			for We	bSphere N	<i>Aessage</i>	m.co	m/suppo	ort WE	BSP-
				allows di	0		view.wss		)217/247
				s which co			wg21995		,
				se sensitiv		4	0		
				ation to th					
			attack						
				RENCE: CV	E-2016-				
			6080		2 2010				
Websphere Mq J	ms		0000					<b>I</b>	
WebSphere MQ c		Message	Service	(WehSnh	ere MO c	lasses fo	or IMS) is	the IMS	nrovider
that is supplied w			001 1100	(Webbph		105565 10	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	ene juie	provider
Execute Code	15-02-2017	7.5	IBM W	ebsphere	MOIMS	http	://www-	Δ_Ι	BM-
Incoute douc	10 02 2017	/.0		7.1, 7.5, 8.0		-	om.com/s		BSP-
				provides c			t/docviev		)217/248
				eserialize o			uid=swg		217/240
				ntrusted s	,	9834	-	21	
				could allo		2034	137		
				ous user to					
				ary Java co	-				
				, vulnerab					
			to the classpath. IBM Reference #: 1983457.						
			REFEF	RENCE: CV	E-2016-				
CV									
		7 2	3-4		56	6-7	7-8	8-9	0 10
Scoring 0-1	1-2	2-3	3-4	4-5	5-6	0-7	7-0	0-9	9-10

			0360								
Imagemagick											
Imagemagick											
ImageMagick is a											
Denial of Service	15-02-2017	4.3	function Magich access 7.0.3.0 attacke of serv read an crafted vendor issue a suppor	The IsPixelMonochrome function in MagickCore/pixel- accessor.h in ImageMagick 7.0.3.0 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted file. NOTE: the vendor says "This is a Q64 issue and we do not support Q64." <b>REFERENCE: CVE-2016-</b>			redh	//bugzi at.com/s ug.cgi?id 694	h	A-IM. IMAC 2802	
Jappix Project	I										
Jappix											
	tured XMPP	web-clien	t (Jappix	Desktop, l	appix Mo	obile	& Ja	opix Min	i).		
NA	09-02-2017			÷ ÷			NA		,	A-JAI	) <u> </u>
			0280: in mul allows to imp includi vulner display variou engine CVE is 1.1.6.	<b>REFERENCE: CVE-2017-</b>						JAPP	
Jasper Project											
Jasper											
Jasper is an open	source platfo		veloping	always-or	n, voice-c					s.	
Overflow	15-02-2017		Stack-l overflo jpc_tsf functio JasPer	Stack-based buffer overflow in the jpc_tsfb_getbands2 function in jpc_tsfb.c in JasPer before 1.900.30 allows remote attackers to			https: om/n asper 1abc2 bf1d5	//githul ndadams /commi 2e5a401 6ca4df91 6df111f4	o.c 5/j t/ a4 3	A-JAS JASP	
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6	-7	7-8		8-9	9-10

_			via a c	nspecified rafted ima <b>RENCE: CV</b>	ge.	5				
Jenkins										
<i>Extra Columns F</i> NA	Plugin									
Cross Site Scripting	09-02-2017	4.3	vulner Colum 1.17 ir remote arbitra HTML failure throug marku	site script ability in t ns plugin Jenkins a e attackers ary web sc by leverag to filter to gh the conf p formatto <b>RENCE: CV</b>	the Extra before llows s to inject ript or ging pol tips figured er.	kin ci. EC ns vis	tps://wiki.jo ns- org/display CURITY/Jenl SHSecurity+A Sory+2016- I-11	/S <i< td=""><td>A-JEN- EXTRA- 280217/252</td></i<>	A-JEN- EXTRA- 280217/252	
Image Gallery P										
Image Gallery is										
Directory Traversal	09-02-2017	5	vulner Gallery in Jenh attacke directe arbitra unspec	ory traver ability in t y plugin be kins allows ers to list a ories and r ary files via cified form <b>RENCE: CV</b>	the Image efore 1.4 s remote arbitrary read a n fields.	e kin ci. EO ns vis 06	tps://wiki.jo ns- org/display CURITY/Jenl SHSecurity+A Sory+2016- 5-20	/S <i< td=""><td>A-JEN- IMAGE- 280217/253</td></i<>	A-JEN- IMAGE- 280217/253	
Tap Plugin		c 1.				1				
Tom's Audio Pro Directory Traversal	09-02-2017	5	Direct vulner plugin Jenkin attack files vi param	ory traver ability in t before 1.2 s allows re ers to reac a an unsp	sal the TAP 25 in emote l arbitrar ecified	ht kin ci. EC y ns vis 06	rm. tps://wiki.jo org/display CURITY/Jenl s+Security+A sory+2016- 5-20	/S <i< td=""><td>A-JEN-TAP P- 280217/254</td></i<>	A-JEN-TAP P- 280217/254	
Jenkins-ci										
<b>Build Failure Analyzer</b> The Build Failure Analyzer plugin lets you set regular expressions for categorizing current and future										
CV 0-1 Scoring Scale	coring 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10									

builds.									
Cross Site Scripting	09-02-2017	4.3	vulner Failure before allows inject a or HTM unspec	Cross-site scripting (XSS) vulnerability in the Build Failure Analyzer plugin before 1.16.0 in Jenkins allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter. <b>REFERENCE: CVE-2016-</b> <b>4988</b>			s://wiki.jer - g/display/S RITY/Jenki Gecurity+Ad ry+2016- 0	BÚII 5 2802	
Jitsi									
<b>Jitsi</b> Jitsi - Open Sour					lls, confer	encing,	chat, deskt	op sha	ring, file
transfer, suppor	09-02-2017	4.3	An ince impler 0280: in mult allows to imp includi vulner display variou engine CVE is 2.9.554	orrect nentation Message ( tiple XMP a remote ersonate a ing contac able appli y. This allo s kinds of ering atta for Jitsi 2.	Carbons" P clients attacker any user, ets, in the ication's ows for social icks. This .5.5061 -	NA			Г-JITSI- 217/256
Kabona Ab									
Webdatorcentro 'WDC' (WebDato cooling and vent	orCentral), a w	eb-based	l unit fo	r monito	ring and	operatio	on of syste	ms for	heating,
Cross Site Scripting	13-02-2017	4.3	Kabon WebDa applica Versio server sanitiz may al scripti	unit for monitoring and o An issue was discovered in Kabona AB WebDatorCentral (WDC) application prior to Version 3.4.0. The web server URL inputs are not sanitized correctly, which may allow cross-site scripting vulnerabilities. <b>REFERENCE: CVE-2016-</b> 8356					AB- 3DA- 217/257
CV Scoring Scale	1 1-2	2-3	3-4	<b>4-</b> 5	5-6	6-7	7-8	8-9	9-10

NA	13-02-2017	5.8	An issue was discovered in Kabona AB WebDatorCentral (WDC) application prior to Version 3.4.0. This non- validated redirect/non- validated forward (OPEN REDIRECT) allows chaining with authenticated vulnerabilities. <b>REFERENCE: CVE-2016- 8376</b>	NA	A-KAB- WEBDA- 280217/258
Knot Dns Projec	t			l	
Knot Dns					
Knot DNS is an op Denial of Service	pen-source serv 09-02-2017	rer progr 5	am for the Domain Name Sys Knot DNS before 2.3.0 allows remote DNS servers to cause a denial of service (memory exhaustion and slave server crash) via a large zone transfer for (1) DDNS, (2) AXFR, or (3) IXFR. <b>REFERENCE: CVE-2016-</b> <b>6171</b>	tem. https://gitlab.la bs.nic.cz/labs/k not/issues/464	A-KNO- KNOT - 280217/259
Lepton Project					
Lepton					
					A-LEP-
Denial of Service	02-02-2017	4.3	lepton/jpgcoder.cc in Dropbox lepton 1.0 allows remote attackers to cause denial of service (out-of- bounds read) via a crafted jpeg file. <b>REFERENCE: CVE-2016-</b> 6238	Dropbox lepton 1.0 allows remote attackers to cause denial of service (out-of- bounds read) via a crafted peg file. <b>REFERENCE: CVE-2016-</b>	
Denial of Service	02-02-2017	4.3	The build_huffcodes function in lepton/jpgcoder.cc in Dropbox lepton 1.0 allows remote attackers to cause denial of service (out-of-	https://github.c om/dropbox/le pton/issues/26	A-LEP- LEPTO- 280217/261
CV Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

			crafted	s write) vi l jpeg file. <b>RENCE: CV</b>					
Denial of Service	02-02-2017	4.3	function lepton Dropb remote a denia bound jpeg fil	The setup_imginfo_jpg function in lepton/jpgcoder.cc in Dropbox lepton 1.0 allows remote attackers to cause a denial of service (out-of- bounds read) via a crafted jpeg file. <b>REFERENCE: CVE-2016-</b>			s://githul /dropbox/ n/issues/2	le LE	LEP- PTO- 0217/262
Denial of Service	02-02-2017	4.3	function lepton Dropb remote a denia (segme crafteo <b>REFEF</b> 6235	/jpgcoder ox lepton e attackers al of servic entation fa l jpeg file. <b>RENCE: CV</b>	.cc in 1.0 allow s to cause ce ault) via a <b>TE-2016-</b>	om/ ptor	s://githul /dropbox/ 1/issues/2	(le LE) 26 28(	LEP- PTO- 0217/263
Denial of Service	02-02-2017	4.3	in lept Dropb remote a denia via a c	ocess_file on/jpgcod ox lepton e attackers al of servic rafted jpeg <b>RENCE: CV</b>	ler.cc in 1.0 allow s to cause ce (crash) g file.	om/ s ptor	s://githul /dropbox/ n/issues/2	'le LE	LEP- PTO- 0217/264
Libav		<u> </u>	0101						
<i>Libav</i> Libav is a free s handling multir	oftware project, nedia data.	forked fi	rom FFm	peg in 201	l1, that p	roduces	libraries	and pro	grams for
Denial of Service	15-02-2017	4.3	get_bit allows cause a (NULL derefe a craft this iss	The get_vlc2 function in get_bits.h in Libav 11.9 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted mp3 file. NOTE: this issue exists due to an incomplete fix for				LIE	LIB- BAV- 0217/265
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			8675.	ENCE: CV RENCE: CV					
Denial of Service	15-02-2017	4.3	get_bit 11.9 al attacke of serv derefe a crafte related sequer detecti	t_vlc2 fun s.h in Liba lows remo ers to caus ice (NULL rence and ed mp3 fil l to startco nces durin on. <b>EENCE: CV</b>	av before ote se a denia pointer crash) vi e, possibl ode g m4v	om/l /com l 9725 931c a 7cbb	s://githul libav/liba nmit/e5b 5f53b791 l3a73171 fd0860	iv LI 01 28 59	-LIB- IBAV- 30217/266
Denial of Service	15-02-2017	4.3	function Libav 2 attacked of serv error a crash) file.	r_make_f_ on in aacst 1.7 allow ers to caus ice (divido nd applica via a craft <b>RENCE: CV</b>	or.c in s remote se a denia e-by-zero ation ced mp3	.org/ t;a=b bavc r.c;h 5b40 b17a 5b91 fb16 531e 7ccf b=a5 a824 2bb9 d52; f589 b4d9	s://git.lib (?p=libav. olobdiff;f= odec/aac =7d156e! 0b197c38 ocf167308 e56;hp=0 77813ce6 e4362d0b 0fdfdd286 0a5ff29e e3499769 0b5509ce hpb=f556 1daf3d53 01763719 0d68fa	gi LI =li 28 sb 52 52 54 64 64 65 65 66 65 66 62 76 96 97 88	-LIB-  BAV- 30217/267
Denial of Service	15-02-2017	4.3	function in Liba remote a denia memote via a cr NOTE: origina	The ff_put_pixels8_xy2_mmx function in rnd_template.c in Libav 11.7 allows remote attackers to cause a denial of service (invalid memory access and crash) via a crafted mp3 file. NOTE: this issue was originally reported as involving a NULL pointer		l		LI	-LIB- BAV- 30217/268
CV Scoring Scale	0-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			dereference. REFERENCE: CVE-2016- 7477		
Denial of Service; Overflow	15-02-2017	4.3	Stack-based buffer overflow in the aac_sync function in aac_parser.c in Libav before 11.5 allows remote attackers to cause a denial of service (out-of- bounds read) via a crafted file. <b>REFERENCE: CVE-2016-</b> <b>7393</b>	https://git.libav .org/?p=libav.gi t;a=commit;h=f b1473080223a 634b8ac2cca48 a632d037a0a6 9d	A-LIB- LIBAV- 280217/269
Denial of Service; Overflow	15-02-2017	4.3	Heap-based buffer overflow in the ff_audio_resample function in resample.c in libav before 11.4 allows remote attackers to cause a denial of service (crash) via vectors related to buffer resizing. <b>REFERENCE: CVE-2016-</b> 6832	https://git.libav .org/?p=libav.gi t;a=commit;h=0 ac8ff618c5e6d8 78c547a8877e7 14ed728950ce	A-LIB- LIBAV- 280217/270
Libavformat Pro	oject				
	f) is a library fo	r dealing	with various media containe	r formats.	
Denial of Service	03-02-2017	4.3	The avcodec_decode_audio4 function in libavcodec in libavformat 57.34.103, as used in MPlayer, allows remote attackers to cause a denial of service (out-of- bounds read) via a crafted mp3 file. <b>REFERENCE: CVE-2016-</b> <b>5115</b>	https://trac.mp layerhq.hu/tick et/2298	A-LIB- LIBAV- 280217/271
Denial of Service; Overflow	03-02-2017	4.3	Integer overflow in the demuxer function in libmpdemux/demux_gif.c in Mplayer allows remote attackers to cause a denial of service (crash) via large dimensions in a gif file.	https://trac.mp layerhq.hu/tick et/2295	A-LIB- LIBAV- 280217/272
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

			REFEF 4352	RENCE: CV	Æ-2016-						
Libdwarf Projec	t										
<i>Libdwarf</i> Libdwarf is a C DWARF3.	library intend	ed to si	mplify	reading (a	and writ	ing)	app	lications	us	ing D	WARF2,
Denial of Service	13-02-2017	4.3	earlier attacke of serv derefe a debu marke file.	rf 201511 allows re ers to caus ice (NULL rence and g_abbrev d NOBITS RENCE: CV	o 1 / 1 1 1 1 1 7 7	om/to /libdv nit/1 Be529	//githul omhugh warf/con 1750a2 953013¢ 953013¢ 97	es n 83 :3	A-LII LIBD 2802		
Denial of Service	15-02-2017	4.3	e funct in libd earlier attacke of serv read) l dwarfe a craft	get_abbr ion in dw warf 2016 allows re ers to caus ice (out-o by calling t lump com ed file. <b>RENCE: CV</b>	arf_util.c 51001 and mote se a denia f-bounds the mand on	od .1 o d 1	redha	//bugzi at.com/s ug.cgi?id 690	sh	A-LII LIBD 2802	
Denial of Service	15-02-2017	4.3	e funct in libd earlier attacke of serv read) l dwarfe a craft	get_abbr ion in dw warf 2016 allows re ers to caus ice (out-o by calling lump com ed file. <b>RENCE: CV</b>	arf_util.c 51001 and mote se a denia f-bounds the mand on	od o v d 6 1 al 0 c f f b b e	orge.i warf/ 58c1f 12af3 0076 2/tree /dwa ff=0b 50d98	//sourc net/p/lil code/ci 18d1d2 b72d7cc b1b88e5 e/libdwa rf_util.c? 28b923d 27d1d9( abadde4	od /2 86 67 61 arf di :3 04f	A-LII LIBD 2802	
Denial of Service	15-02-2017	4.3	The _dwarf_get_size_of_val function in libdwarf/dwarf_util.c in Libdwarf before 20161124 allows remote			al h .1 0 1	nttps: redha	://bugzi at.com/s ug.cgi?id 689	sh	A-LII LIBD 2802	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8		8-9	9-10

			of serv read) l dwarfo a craft	ers to caus ice (out-o by calling t lump com ed file. <b>RENCE: CV</b>	f-bounds the mand on					
Libtiff										
<i>Libtiff</i> Libtiff is a library	for reading and	d writing	Tagged	Image Fil	e Format	(abbre	eviated TIF	F) file	es.	
Denial of Service; Overflow	06-02-2017	4.3	Buffer readgi gif2tiff in Lib7 remote a denia (segme craftee	overflow fimage fur fir the gi TFF 4.0.6 e attackers al of servic entation fa l gif file. <b>RENCE: CV</b>	in the action in if2tiff tool allows s to cause ce ault) via a	htt ma l hov =2!	p://bugzill ptools.org w_bug.cgi? 552	la. // /s I	A-LIB LIBTI	
Libtorrent								<b>I</b>		
Libtorrent										
libtorrent is a fea	ture complete (	C++ bitto	rrent im	plementa	tion focus	sing on	efficiency	and s	calab	oility.
Denial of Service	07-02-2017	5	puff.cp 1.1.0 a torren denial (segme crash) respor	nstruct fu p in Libto llows rem t trackers of service entation fa via a craft ise. <b>RENCE: CV</b>	rrent ote to cause a ault and ced GZIP	om orr	ps://githu /arvidn/li ent/pull/1	bt I	A-LIB LIBT( 2802	
Libxpm Project										
<i>Libxpm</i> LibXpm provides used in legacy X a	pplications.		-		-	-				
Denial of Service; Execute Code; Overflow	01-02-2017	7.5	in libX when a parsin on a 64 remote a denia	le integer pm before a program g XPM ext 4-bit platfo e attackers al of servio s write) on	3.5.12, requests ensions orm, allov s to cause ce (out-of	des rg/ om v 674 7f6	ps://cgit.fr sktop.org/2 /lib/libXpn mit/?id=d 418f0fd02a 517ec5afd6 53afbe185	xo   I n/c   2 11 a2 5d	A-LIB LIBXF 2802	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-'	9	9-10

			numbe (2) the length file, wh based	ry code v r of exten ir concate in a crafte ich trigge buffer ove ENCE: CV	sions or enated ed XPM ers a heap erflow.	)-			
Lynxspring									
Jenesys Bas Brid The JENEsys Bui management, en these challenges	ilding Operating tergy managem	ent, and	facility	usage an	d techno	ology n	anagemer	nt, and	addresses
or large institution		-			•	-	-		
NA	13-02-2017	5	Lynxsp Bridge older. ' databa safegu creden	ie was dis oring JENE versions Γhe applic se lacks s ards for p tials. E <b>ENCE: CV</b>	Esys BAS 1.1.8 and cation's ufficient rotecting			JI	-LYN- ENES- 80217/280
NA	13-02-2017	5.5	Lynxsp Bridge older. A only ac comma and the accept This w attacke access within	te was dis pring JENE versions A user wit cess can s ands to th e applicat those com ould allow er with res to make c the applic ENCE: CV	Esys BAS 1.1.8 and th read- send e softwar ion will nmands. v an ad-only thanges cation.	e		JI	-LYN- ENES- 80217/281
Cross Site Request Forgery	13-02-2017	6.8	An issu Lynxsp Bridge older.' does n if a req intenti	ie was dis pring JENF versions The applic ot sufficie uest was onally pro er who sul	Esys BAS 1.1.8 and cation ntly verif ovided by	ý		JI	-LYN- ENES- 80217/282
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

				REQUI	quest (CRC EST FORGI <b>RENCE: CV</b>	ERY).				
NA	13	3-02-2017	7.5	Lynxsp Bridge older. a hard with n allowin the sys auther	ue was dis pring JENE versions The applic -coded use o passwor ng an attao stem witho ntication. <b>RENCE: CV</b>			JEN	YN-  ES- )217/283	
Mariadb;Ora	acle									
Mariadb/My	vsql									
MariaDB is a										
intended to management			ler the	GNU GP	'L/ MySQ	L is an	open-so	ource re	lational	database
NA		L-02-2017	5	in Orac 5.6.21 5.7.5 a throug throug 10.2.x	in libmysq cle MySQL and 5.7.x nd MariaE (h 5.5.54, 1 (h 10.0.29, (h 10.1.21, through 1 <b>RENCE: CV</b>	before before DB 10.0.x 10.1.x and 0.2.3.	enwa s/os secu	//www.o all.com/li s- rity/201′ .1/11	ist MA 280	1AR- RIA- )217/284
Mcabber										
<i>Mcabber</i> MCabber is a based on ncu		oftware clie	ent for th	e instant	t messagir	ig protoco	ol XMPP	with a t	ext user	interface
NA		9-02-2017	4.3	0280: in mul allows to imp includ: vulner display variou	orrect nentation Message C tiple XMP a remote ersonate a ing contac rable appli y. This allo s kinds of eering atta	NA		MC	1CA- ABB- 0217/285	
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			1.0.4.	for mcabb RENCE: CV					
Mcafee									
<b>Epolicy Orchestr</b> McAfee ePolicy O security manager	rchestrator (M			e most ad	vanced, e	xtensibl	e, and sca	lable cer	tralized
Cross Site Scripting; Bypass	13-02-2017	3.5	vulner user in Securit 5.1.1, a authen inject i scripts validat	site script ability in t terface (U ty ePO 5.1 and 5.1.0 a ticated us nalicious via bypas tion. <b>ENCE: CV</b>	the Web II) in Inte .3, 5.1.2, Illows sers to Java ssing inpu	ee.co l te/ir cont 1018	s://kc.mca om/corpor ndex?page ent&id=SF 34	ra EPO = 2802	
Modified									
<b>Ecommerce Shop</b> NA	osoftware	_							
Execute Code; SQL Injection	15-02-2017	7.5	vulner eComn 2.0.0.0 when t is not i remote execut comma orders custom param api/ea hp.	le SQL inje abilities ir nerce Shoj revision 9 che easybi nstalled, a e attackers e arbitrary ands via th _status or ners_statu eter to sybill/eas	n modifie psoftwar 9678, Il-module Illow s to y SQL ne (1) (2) s ybillcsv.p	e		A-M0 EC0 2802	
Movim									
<i>Movim</i> MOVIM is a distri protocol.	buted social n	etwork b	uilt on to	op of XMP	P, a popu	lar open	standards	s commu	nication
NA	09-02-2017	4.3	-	orrect nentation Message C		NA		A-M0 MOV 2802	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			allows to imp includi vulner display variou engine CVE is 0.10.	tiple XMP a remote ersonate a ing contac able appli 7. This allo s kinds of ering atta for Movin RENCE: CV	attacker any user, ts, in the cation's ows for social cks. This n 0.8 -				
Moxa									
<b>Dacenter</b>	log o stordard	ODC inte	nfo oc the	tintoract	a with M			muca fa	n nool time
DA-Center provid data collection.	les a standard	OPC inte	rrace tha	it interacts	s with Mo	oxa Acti	ve OPC Se	erver fo	r real-time
NA	13-02-2017	4.6	Moxa I 1.4 and applica from a path is	ie was dis DACenter <sup>*</sup> d older. Th ation may n unquote sue. <b>RENCE: CV</b>	Versions ie suffer ed search			D	-MOX- ACEN- 30217/289
NA	13-02-2017	7.1	Moxa I 1.4 and crafted cause t crash b Uncom Consu	te was dis DACenter ' d older. A s project fi the progra because of trolled Re mption. <b>RENCE: CV</b>	Versions specially le may im to source			D	-MOX- ACEN- 30217/290
Softcms			7551						
SoftCMS is a point installations in a second		2.	gement	software	solution	that n	nanages	large s	cale CCTV
SQL Injection	13-02-2017	6.5	Moxa S prior t SoftCM not pro that m attacke	ie was dis SoftCMS ve o Version IS Applica operly san ay allow a er access t dministrat	it		S	-MOX- DFTC- 30217/291	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

				crafted INJECT	ge throug l input (SC FION). <b>RENCE: CV</b>	)L	-				
Denial of Service; Execu Code		3-02-2017	7 6.8	Moxa S prior t specia reques SoftCM can ca condit allowin modify and po denial execut code.	ue was dis SoftCMS version Ily crafted st sent to t IS ASP We use a doub ion on the ng an attac y memory ossibly cau of service ion of arb RENCE: CV	ersions 1.6. A URL he observer ole free server cker to locations ise a or the itrary	;			A-MC SOFT 2802	
NA	1	3-02-2017	7 7.8	Moxa S prior t SoftCM not provid and ca crash o consul service	ue was dis SoftCMS ve o Version IS Webser operly vali An attacke le unexpec use the pr or excessiv nption of result in a e condition <b>RENCE: CV</b>	ersions 1.6. Moxa ver does idate er could er could cted value ogram to ve resources denial-of n.	es 5 5-			A-MC SOFT 2802	
Msweet											
<i>Mini-xml</i> Mini-XML is a application wi							XML ar	ıd XML-liko	e da	ta files	in your
Denial of Service		3-02-2017		The mxml_write_node function in mxml-file.c in mxml 2.9, 2.7, and possibly earlier allows remote attackers to cause a denial of service (stack			.re ow 13	ps://bugzi dhat.com/: _bug.cgi?ic 34648	sh	A-MS MINI 2802	
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8-9	9-10

CV Scoring Scale	1-2	2-3	<b>3-4</b>	<b>4-5</b>	5-6	6-7			8-9	9-10
multi-tenant billi		-	The Da compo OnCon		ouse etApp sight	htt pp t/s	ps://kb.r .com/sup /article/ 20170131	neta opor NTA	A-NE ONCO	- T-
<b>Oncommand Ins</b> OnCommand Insi	•	enterpr	ise-custo	omers man	nage capa	icity. n	erforman	ice. fo	recast	ing, and
			unspeo	ation via cified vect RENCE: CV		00	01			
Information		5	ONTAI allows obtain	P before 8. remote at SMB shar	.3.2P7 tackers t	o t/s P-2	.com/sup s/article/ 20161028	por NTA	CLUS	-
<b>Clustered Data C</b> Clustered Data O so your operation Gain	NTAP provides	-	0	controlle p Clustere			naged as		<mark>gle logi</mark> A-NE	
Netapp			10009	•						
			link at init sci CVE-20	rivileges v tack on th tipt file, re 016-8641. <b>RENCE: CV</b>	e Nagios lated to				2802	17/296
Nagios provides applications mon Gain Privileges	-	7.2	Nagios	4.2.4 and	earlier	NA		LOLIUE	A-NA	G-
Nagios	ontonnico da	na Onan	Course	IT mon	itoring	noturo	rle monit	toring		on and
Nagios			4570							
Denial of Service	03-02-2017	7.1	xml file REFER 4571 The main in mxm 2.9, 2.7 earlier attacke of serv consum xml file	e. RENCE: CV xmlDelete nl-node.c i 7, and poss allows re ers to caus rice (stack nption) vi	<b>E-2016</b> function in mxml sibly mote se a denia a crafted	htt .re ow 13 I	ps://bug dhat.com bug.cgi? 34648	/sh	A-MS MINI 2802	
				nption) vi	a crafted					

			attackers to obtain administrative access by leveraging a default privileged account. <b>REFERENCE: CVE-2017-</b> <b>5600</b>	0001	
<b>Oncommand Sys</b> OnCommand Sys storage systems.	stem Manager p	orovides	fast, simple configuration ar	nd management fo	r NetApp FAS
Execute Code	07-02-2017	4.4	Multiple functions in NetApp OnCommand System Manager before 8.3.2 do not properly escape special characters, which allows remote authenticated users to execute arbitrary API calls via unspecified vectors. <b>REFERENCE: CVE-2016-</b> <b>3063</b>	https://kb.neta pp.com/suppor t/s/article/Refe rence: CVE- 2016-3063- zapi-injection- vulnerability- in-oncommand- system- manager	A-NET- ONCOM- 280217/299
	ified Manager 1		t <b>ered Data Ontap</b> and alerts on the health o	f your NetApp sto	orage running
Execute Code	07-02-2017	7.5	NetApp OnCommand Unified Manager for Clustered Data ONTAP 6.3 through 6.4P1 contain a default privileged account, which allows remote attackers to execute arbitrary code via unspecified vectors. <b>REFERENCE: CVE-2016-</b> <b>6667</b>	https://kb.neta pp.com/suppor t/s/article/NTA P-20161017- 0002	A-NET- ONCOM- 280217/300
• •	ommand Work	flow Aut	omation solution improves p	productivity in you	r organization
by automating st Bypass	orage-managen 07-02-2017	9.3	NetApp OnCommand Workflow Automation before 3.1P2 allows remote attackers to bypass authentication via unspecified vectors. <b>REFERENCE: CVE-2016-</b> <b>1894</b>	https://kb.neta pp.com/suppor t/s/article/Refe rence: CVE- 2016-1894- authentication- bypass- vulnerability-	A-NET- ONCOM- 280217/301
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

						wor	ncomman kflow- omation	d-	
Snap Creator F	ramework								
	dent NetApp Sna				es with Ne	etApp u	nified data	a prot	ection
	d delivers applic								
Cross Site Request Forgery	07-02-2017	6.8	Cross-site request forgery (CSRF) vulnerability in NetApp Snap Creator Framework before 4.3.0P1 allows remote attackers to hijack the authentication of users for requests that have unspecified impact via unknown vectors. <b>REFERENCE: CVE-2016-</b> 5372			pp.c t/s/ 1 rend o 201 cros requ forg vulr in-s crea	ierability- nap-	or S efe 2	A-NET- NAP - 80217/30
Snapcenter Ser						fran	iework		
SnapCenter pro manage applica	nter Software is ovides centralize tion-specific bac	ed contro kup, rest	ol and ore, and	oversight, clone job	while d s.	elegatin	g the abi	ility f	or users t
Bypass	07-02-2017	7.5	1.0 and remote partial auther list and unspec	p SnapCer d 1.0P1 all e attackers ly bypass ntication a d delete ba cified vect <b>RENCE: CV</b>	ows s to nd then ackups vi ors.	pp.c t/s/ enti byp a vulr in-s	s://kb.net om/suppo article/au cation- ass- nerability- napcenter ver-1-0-1-	or S ith 2	A-NET- NAPC- 80217/30
	ive for Microsof tual environmer		ws imp	roves IT	efficiency	y and a	utomates	data	storage i
Gain Information	07-02-2017	5	NetApp SnapDrive for Windows before 7.0.2P4, 7.0.3, and 7.1 before 7.1.3P1 allows remote attackers to obtain sensitive information via unspecified vectors. <b>REFERENCE: CVE-2015-</b> <b>8544</b>				s://kb.net om/suppo article/Re ce: CVE- 5-8544- sitive- rmation- losure-in- odrive-for- dows	or S efe 2	A-NET- NAPD- 80217/30
CV 0- Scoring Scale	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Virtual Storage (									
NetApp Virtual S				Sphere i	mproves	efficien	cy and r	educe	s cost and
complexity in a V									
NA	07-02-2017	6.8	Consol vSpher a non which attacke in-the- unspec	p Virtual S e for VMw re before 6 unique cer allows ren ers to cono middle at cified vect <b>ENCE: CV</b>	pp.c t/s/ P-20 000	s://kb.net om/suppo article/NT 0161108- 1	or V	NET- 'IRTU- 80217/305	
Nitro Software									
Nitro Pro With Nitro Pro yo	ou can open, rev	view, cov	vert and o	create PD	F files.				
Memory Corruption	10-02-2017	6.8	A remo write / corrup exists i functio 10.5.9. crafted a vulne potent corrup can sen specifi this vu	ote out of l memory tion vulne n the PDF onality of l 9. A special PDF file erability re ial memori tion. An a nd the vict c PDF file lnerability <b>ENCE: CV</b>	bound erability F parsing Nitro Pro ally can cause esulting in ry ttacker ttacker tim a to trigger y.	osin om/ LOS 0220	://www.ta telligence. reports/T -2016- 6/	c N	-NIT- IITRO- 80217/306
Execute Code	10-02-2017	6.8	A pote execut exists i functio 10. A s file car vulner potent An atta victim trigger	ntial remo ion vulner n the PDF onality of I pecially of a cause a ability res ial code ex acker can a specific this vulne <b>ENCE: CV</b>	osin om/ LOS 022	://www.ta telligence. reports/T -2016- 4/	c N	-NIT- IITRO- 80217/307	
Overflow;	10-02-2017	6.8	A remote out of bound http://www.				://www.ta	al A	-NIT-
CV 0-1 Scoring Scale	1-2	2-3	<b>3-4 4-5 5-6</b>				7-8	8-9	9-10

Memory			write / memory	osintelligence.c	NITRO-
Corruption			corruption vulnerability exists in the PDF parsing functionality of Nitro Pro 10. A specially crafted PDF file can cause a vulnerability resulting in potential memory corruption. An attacker can send the victim a specific PDF file to trigger this vulnerability. <b>REFERENCE: CVE-2016-</b> 8709	om/reports/TA LOS-2016- 0218/	280217/308
NInetlabs	-			L	
<i>NSD</i> In Internet com (DNS) server.	nputing, NSD (for	r "name	server daemon") is an ope	n-source Domain	Name System
Denial of Service	09-02-2017	7.8	NSD before 4.1.11 allows remote DNS master servers to cause a denial of service (/tmp disk consumption and slave server crash) via a zone transfer with unlimited data. <b>REFERENCE: CVE-2016-</b> <b>6173</b>	http://www.nln etlabs.nl/svn/n sd/tags/NSD_4_ 1_11_REL/doc/ RELNOTES	A-NLN-NSD- 280217/309
Nvidia					
accelerate deep accelerators nov and small-and-	learning, analyti w power energy medium busine	ics, and e -efficient sses arc	f a graphics processing unit ngineering applications. Pion data centers in governmen ound the world. They play tificial intelligence to cars, dr	neered in 2007 by It labs, universities 7 a huge role in	NVIDIA, GPU s, enterprises accelerating
Denial of Service	15-02-2017	4.9	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer handler where improper handling of values may cause a denial of service on the system. <b>REFERENCE: CVE-2017- 0320</b>	http://nvidia.cu sthelp.com/app /answers/detai l/a_id/4398	A-NVI-GPU D- 280217/310

0320

3-4

4-5

5-6

6-7

7-8

8-9

9-10

CV

Scoring Scale 0-1

1-2

2-3

Denial of Service	15-02-2017	4.9	Windo Driver vulner: mode l improp values of serv	sions of N ws GPU D contain a ability in f ayer hand oer handli may caus ice on the ENCE: CV	isplay the kerne ller wher ing of e a denial system.	st  /a    / e 	thelp answ	/nvidia. .com/aj ers/det /4398	рр	p D- ai 280217/3		
Denial of Service	15-02-2017	4.9	Linux ( contain the ker handle validat paramo denial system	sions of N GPU Displ n a vulner rnel mode r where in ion of an eter may of service ENCE: CV	ay Driver ability in layer mproper input cause a on the	st /: //	thelp answ	/nvidia .com/aj rers/det /4398	рр	D-	I-GPU 17/312	
Denial of Service	15-02-2017	4.9	GPU Di contain the ker handle access unpriv a denia	sions of N splay Dri n a vulner rnel mode r where in controls a ileged use il of servie ENCE: CV	ver ability in layer mproper allowing er to caus ce.	st /a l/	thelp answ	/nvidia .com/aj ers/det /4398	рр	D-	I-GPU 17/313	
Execute Code	15-02-2017	6.9	All vers GPU an Experie contain where permis packag thus al priviles with th potent escalat code est	sions of N ad GeForc ence insta a vulner it fails to sions on e extracti lowing a ged user t e extract ially leadi ion of pri kecution.	e aller ability set prope the on path non- to tamper ed files, ng to vileges vi	st // l/ r	thelp answ	/nvidia .com/aj ers/det /4398	рр	D-	I-GPU 17/314	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8		8-9	9-10	

			0317		
Denial of Service; Overflow	15-02-2017	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where the size of an input buffer is not validated, leading to denial of service or potential escalation of privileges. <b>REFERENCE: CVE-2017- 0324</b>	http://nvidia.cu sthelp.com/app /answers/detai l/a_id/4398	A-NVI-GPU D- 280217/315
Denial of Service	15-02-2017	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer handler where a NULL pointer dereference caused by invalid user input may lead to denial of service or potential escalation of privileges. <b>REFERENCE: CVE-2017- 0323</b>	http://nvidia.cu sthelp.com/app /answers/detai l/a_id/4398	A-NVI-GPU D- 280217/316
Denial of Service	15-02-2017	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler where a value passed from a user to the driver is not correctly validated and used as the index to an array, leading to denial of service or potential escalation of privileges. <b>REFERENCE: CVE-2017- 0322</b>	http://nvidia.cu sthelp.com/app /answers/detai l/a_id/4398	A-NVI-GPU D- 280217/317
Denial of Service	15-02-2017	7.2	All versions of NVIDIA GPU Display Driver	http://nvidia.cu sthelp.com/app	A-NVI-GPU D-
CV Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

CV											
Denial of Service;	1	5-02-2017	7.2		sions of N ws GPU D		_	elp.com/ap		A-NV D-	I-GPU
Denial of Service; Overflow	1	5-02-2017	7.2	Windo Driver vulner mode (nvldd impler Submi DDI (Dxgkl Virtua input i memo intend buffer service privile	ws GPU D contain a ability in t layer mkm.sys) nentation tComman DdiSubmit l) where u s used to p ry outside ed bounda leading to e or escala	isplay the kernel of the dVirtual cCommane intrusted reference of the ary of the denial of ition of	sthe /an l/a_	e://nvidia. elp.com/ap swers/det id/4398	р	D-	I-GPU 17/320
Denial of Service Denial of		5-02-2017	7.2	0321All verWindoDrivervulnermode(nvlddfor Dxan atterinvaliolead topotentprivileREFEH0315	sions of N ws GPU D contain a ability in t layer mkm.sys) gkDdiEsca empt to ac l object po denial of cial escalat	VIDIA isplay the kernel handler pe where cess an binter may service on cion of <b>/E-2017-</b>	sthe /an l/a_	e://nvidia. elp.com/ap swers/det id/4398	pp ai	D- 2802	I-GPU 17/319 I-GPU
				the ker handle pointe caused input n service escala <b>REFE</b>	n a vulner rnel mode er where a r derefere d by invalie may lead t e or poten tion of pri- <b>RENCE: CV</b>	layer NULL ence d user o denial o tial vileges.	ĺ/a_	swers/det id/4398	ai	2802	17/318

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

Overflow			mode l (nvldd impler Submit DDI (DxgkI Virtual input i memou intend buffer service privile	gkDdiSubmitCommand cual) where untrusted ut is used to reference mory outside of the ended boundary of the fer leading to denial of vice or escalation of vileges. FERENCE: CVE-2017- L3 versions of NVIDIA http:/ ndows GPU Display ver contain a				ai	2802	17/321
Denial of Service	15-02-201	17 7.2	Windo Driver vulner mode l (nvldd for Dxg 0x1000 provid the lim lead to potent privile	3 versions of NVIDIA dows GPU Display ver contain a nerability in the kernel de layer ddmkm.sys) handler DxgkDdiEscapeID 00008b where user vided input is used as limit for a loop may to denial of service or ential escalation of			//nvidia. p.com/ap wers/det 1/4398	р	D-	I-GPU 17/322
Denial of Service	15-02-201	17 7.2	NVIDIA Driver vulner mode l improj may le service escalat	IA GPU Display r R378 contains a rability in the kernel layer handler where oper access control ead to denial of ce or possible ation of privileges. <b>RENCE: CVE-2017-</b>		sthel /ans	//nvidia. p.com/ap wers/det 1/4398	р	D-	I-GPU 17/323
Denial of Service; Overflow	15-02-201	7.2	All ver GPU D	sions of N isplay Driv n a vulner	ver	sthel	//nvidia. p.com/ar wers/det	р	D-	I-GPU 17/324
CV 0.1	1 0	2.2	3_1	4.5	5-6	67	78		2 0	9-10

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

Gain Information	13-02-2017	5	password requirements for the OmniView web application may allow a attacker to gain access brute forcing account passwords. <b>REFERENCE: CVE-201</b> <b>5801</b> An issue was discovere OmniMetrix OmniView, Version 1.2. The OmniView web application transmits credentials with the HT protocol, which could b	s an by <b>6-</b> d in NA , TP	A-OMN- OMNIV- 280217/326
			for the OmniView web application may allow a attacker to gain access brute forcing account passwords. <b>REFERENCE: CVE-201</b> 5801	s an by <b>6-</b>	280217/326
		Ĵ	OmniMetrix OmniView, Version 1.2. Insufficient	,	OMNIV-
Omnimetrix Omniview OmniMetrix is th stand-by generate NA			M2M wireless remote r uipment. An issue was discovere		l for pipelines,
Denial of Service; Overflow	15-02-2017	7.2	the kernel mode layer handler where multiple integer overflows may cause improper memor allocation leading to a denial of service or potential escalation of privileges. <b>REFERENCE: CVE-201</b> 0309 All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kern mode layer (nvlddmkm.sys) handle for DxgkDdiEscape whe untrusted input is used buffer size calculation leading to denial of serv or escalation of privileg <b>REFERENCE: CVE-201</b> 0308	7y 7- http://nvidia.cu sthelp.com/app /answers/detai l/a_id/4398 er er er er er er er er er er	A-NVI-GPU D- 280217/325

			may re compr creden	by an atta sult in the omise of a tials. <b>ENCE: CV</b>	e Iccount						
Openafs											
<b>Openafs</b> Coordination and including client a		vare.	FS, an op	ensource	impleme	entat	tion o	of the An	drev	w File	System,
Gain Information	06-02-2017	5	earlier attacke sensiti inform involvi cache j fileser (3) cer	FS 1.6.19 allows re ers to obta ve directo ation via v ng the (1) partition, ( ver vice pa tain RPC r <b>EENCE: CV</b>	mote ain ry vectors client (2) artition, c	or s.	pena es/se ENAF	://www fs.org/pa ccurity/( S-SA- -003.txt	ag )P	A-OP OPEN 2802	
Openjpeg											
<b>Openjpeg</b> OpenJPEG is an o	pen-source JPE	<u>G 2000 c</u>	odec wr	itten in C	language	2.				1	
Denial of Service	03-02-2017	4.3	functio commo OpenJI allows cause a (out-of crafted	cc422_t_r on in PEG before remote at a denial of bounds r l jpeg2000 <b>ENCE: CV</b>	in e 2.1.1 tackers t service read) via ) file.	to a	.redh	://bugzi at.com/s ug.cgi?ic 821	sh	A-OP OPEN 2802	
Plone											
<i>Plone</i> Plone is a free a server.	nd open sourc	e conter	it manag	gement sy	vstem bu	ilt o	on toj	p of the	Zoj	be app	lication
Cross Site Scripting	04-02-2017	Cross-site scripting (XSS) vulnerability in the manage_findResult component in the search feature in Zope ZMI in Plone before 4.3.12 and 5.x before 5.0.7 allows				NA			A-PLO PLON 2802		
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6	5-7	7-8		8-9	9-10

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Psi-plus Psi+ Psi+ is a dev C++) design NA	ed for t	ent branch o he Jabber po 09-02-2017		An inc impler 0280: in mul allows to imp includ display		of "XEP- Carbons" P clients attacker any user, ts, in the cation's ows for	NA	powerful	A-PS	lient (Qt, SI-PSI+- 217/332
NA		ninates prof 09-02-2017	anity and 4.3	An inc impler 0280: in mul allows to imp includ vulner display variou engine CVE is - 0.5.0	orrect nentation Message ( tiple XMP) a remote ersonate a ing contac able appli y. This allo s kinds of ering atta for profar	of "XEP- Carbons" P clients attacker any user, ts, in the cation's ows for social cks. This nity (0.4.7	NA	eb.	A-PI PRO 280	
				arbitra HTML involvi as dem obj_ids NOTE: exists incom REFER 7140. <b>REFER</b>	e attackers via vector ing double onstrated stokens p this vulne because of plete fix fo ENCE: CV	ript or s e quotes, l by the arameter erability f an or E-2016-				

	1				
			engineering attacks. This CVE is for Psi+ (0.16.563.580 - 0.16.571.627). <b>REFERENCE: CVE-2017-</b> <b>5593</b>		
Python					
Openpyxl					
	hon library for	reading a	and writing Excel 2010 xlsx/x	lsm/xltx/xltm files	S.
NA	15-02-2017	5.8	Openpyxl 2.4.1 resolves external entities by default, which allows remote attackers to conduct XXE attacks via a crafted .xlsx document. <b>REFERENCE: CVE-2017-</b> <b>5992</b>	https://bugs.de bian.org/cgi- bin/bugreport.c gi?bug=854442	A-PYT- OPENP- 280217/333
Saltstack					
Salt					
Salt is a new appr	roach to infrast	ructure n	nanagement built on a dynam	ic communication	bus.
NA	07-02-2017	7.5	Salt before 2015.8.11 allows deleted minions to read or write to minions with the same id, related to caching. <b>REFERENCE: CVE-2016-</b> <b>9639</b>	https://docs.sal tstack.com/en/ 2015.8/ref/con figuration/mast er.html#rotate- aes-key	A-SAL- SALT- 280217/334
Sanadata				L	
Cross Site Scripting	velops product 04-02-2017		e for eCommerce, eLearning a Cross-site scripting (XSS) vulnerability in index.asp in SANADATA SanaCMS 7.3 allows remote attackers to inject arbitrary web script or HTML via the search parameter. <b>REFERENCE: CVE-2017-</b> 5882	nd Web Content M	anagement. A-SAN- SANAC- 280217/335
SAP					
	•		any SAP system. It consists o zstem and execute the SAP pr		es that run on

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	15-02-2017	5	The SAP Message Server HTTP daemon in SAP KERNEL 7.21-7.49 allows remote attackers to cause a denial of service (memory consumption and process crash) via multiple msgserver/group?group= requests with a crafted size of the group parameter, aka SAP Security Note 2358972. <b>REFERENCE: CVE-2017- 5997</b>				s://erpsca /advisorie scan-16- sap- sage- er-http- ote-dos/	s K-	SAP-SAP 30217/336
Schneider-elect	ric	-	•					•	
<b>Powerlogic Pm8</b> The PM8ECC is connectivity betw clients to access i	a communicat ween Ethernet nformation fro	(Modbu m the ho	s TCP/I st Powe	P) and se r Meter ar	rial line d id the seria	levices, al slave	allowing	Modb	us TCP/IP
NA	13-02-2017	7.5	Schnei Power device Undoc coded access	ae was dis der Electr Logic PM8 2.651 and umented l credential to the dev RENCE: CV	I NA		PC	SCH- DWER- 30217/337	
Simplemachines	5								
Simple Machines Simple Machines community forum	s <b>Forum</b> s offers free c n written in PH	P.	_			the p	owerful a		
Execute Code	09-02-2017	6.8	Machin 2.1 allo attacko object and ex code v variab user in loop.		t (SMF) te duct PHP attacks trary PHP related to d from oreach	om/S hines ssues	s://github. SimpleMac s/SMF2.1/ s/3522	: SI	SIM- MPL- 30217/338
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Execute Code	09-02-2017	7.5	Packages.php in Simple Machines Forum (SMF) 2.1 allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via the themechange array parameter. <b>REFERENCE: CVE-2016-</b> <b>5726</b>		A-SIM- SIMPL- 280217/339
Simplesamlphp					
<i>Simplesamlphp</i> SimpleSAMLphp authentication.	is an award-	winning	application written in	native PHP that	t deals with
Gain Information	07-02-2017	5	The sanitycheck module in SimpleSAMLphp before 1.14.1 allows remote attackers to learn the PHP version on the system via unspecified vectors. <b>REFERENCE: CVE-2016-</b> <b>3124</b>	amlphp.org/sec urity/201603-	A-SIM- SIMPL- 280217/340
Sleekxmpp Proj	ect: Slixmpp P	roiect			
Sleekxmpp/Slixm A common use ca licensed XMPP lik	ase for SleekXM		send one-off messages fror	n time to time/ Slix	mpp is an MIT
NA	09-02-2017	4.3	An incorrect implementation of "XEP- 0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for SleekXMPP up to 1.3.1 and Slixmpp all versions up to 1.2.3, as bundled in poezio (0.8 - 0.10) and other products. <b>REFERENCE: CVE-2017-</b> <b>5591</b>	NA	A-SLE- SLEEK- 280217/341
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

Squidguardit/32b1456e2 3a32c7f45079c 3985bf732dd0d 276dSquidguardEFFERENCE: CVE-2016- 6188A-SQUSquidguard09-02-20174.3Cross-site scripting (XSS) vulnerability in squidGuard.cgi in squidGuard before 1.5 inject arbitrary web script or HTML via a blocked site link.http://www.sq eP14/4 Readm eP14/4 Readm eP14/4 Readm eP14/4 ReadmA-SQU- SQUID- 20150201VideoinsightFFFERENCE: CVE-2015- ag936http://www.sq uidguard.org/D 20150201A-SQU- SQUID- 20150201VideoinsightFFFERENCE: CVE-2015- ag936NAA-VID-WE COTVideoinsightStrong of the specific of the speci	Sogo					
Denial of Service03-02-20176.8 e.8 allows remote attackers to allows remote attackers to cause a denial of service (memory consumption) via a large number of attempts to upload a large 39325745079c 333227450732d001 33322745079c 33322745079c 33322745079c 333227450732d001 33322745079c 33322745079c 33322745079c 3322745070c 343021773 30951732d001 30951732d001 30951732d001 30951732d001 30951732d001 309510732d001 309510732d001 3090102101https://github.c allows remote attackers to inject arbitrary wb script inject arbitrary wb scr		ported and tru	sted grou	upware server with a focus or	n scalability and on	en standards.
Squidguard SquidGuard is URL redirector software which can be used for content control of websites.Cross Site Scripting09-02-20174.3 Cross-site scripting (XSS) vulnerability in squidGuard cgi in squidGuard before 1.5 allows remote attackers to inject arbitrary web script or HTML via a blocked site link. REFERENCE: CVE-2015- 8936http://www.sq uidguard.org/D sQUID- 280217/3VideoinsightWeb Client Cross Site (Intranet, or Internet resource identified by a URI. Execute Code; SQL Injection13-02-20177.5 T An issue was discovered in VideoInsight Web Client VideoInsight Web Client Version 6.3.5.11 and previous versions. SQL Injection REFERENCE: CVE-2017- 5151NAA-VID-WE C- 280217/3VIMVIMVim san advanced text editor that seeks to provide the power of the de-facto Unix editor 'Vi', withVin', with	Denial of			Memory leak in SOGo 2.3.7 allows remote attackers to cause a denial of service (memory consumption) via a large number of attempts to upload a large attachment, related to temporary files. <b>REFERENCE: CVE-2016-</b>	https://github.c om/inverse- inc/sogo/comm it/32bb1456e2 3a32c7f45079c 3985bf732dd0d	A-SOG-
SquidGuard is URL redirector software which can be used for content control of websites.Cross Site Scripting09-02-20174.3Cross-site scripting (XSS) vulnerability in squidGuard.org in squidGuard.org in squidGuard before 1.5 allows remote attackers to inject arbitrary web script or HTML via a blocked site link. REFERENCE: CVE-2015- 8936http://www.sq uidguard.org/D ownloads/Patc hes/1.4/Readm e.Patch- 20150201A-SQU- SQUID- 280217/3VideoinsightKepference: CVE-2015- 8936Mathematical action of receiving data from any loc intranet, or Internet resource identified by a URI.A-VID-WR C- 280217/3Execute Code; SQL Injection13-02-20177.5 SISAn issue was discovered in VideoInsight Web Client Version 6.3.5.11 and previous versions. SQL lipiction vulnerability has been identified, which may allow remote code execution. REFERENCE: CVE-2017- S151NAA-VID-WF C- 280217/3VIMVIMVim is an advanced text editor that seeks to provide the power of the de-facto Unix editor 'Vi', witt	Squidguard				L	
Cross Site Scripting09-02-20174.3Cross-site scripting (XSS) vulnerability in squidGuard.cgi in squidGuard.cgi in squidGuard before 1.5 allows remote attackers to inject arbitrary web script or HTML via a blocked site link. REFERENCE: CVE-2015- 8936http://www.sq uidguard.org/D ownloads/Patc hes/1.4/Readm e.Patch- 20150201A-SQU- SQUID- 280217/3VideoinsightWeb Client The WebClient class provides common methods for sending data to or receiving data from any loo intranet, or Internet resource identified by a URI.MAA-VID-WE C- 280217/3Execute Code; SQL Injection13-02-20177.5An issue was discovered in VideoInsight Web Client Viesion 6.3.5.11 and previous versions. SQL Injection vulnerability has been identified, which may allow remote code execution. REFERENCE: CVE-2017- S151NAA-VID-WE C- 280217/3VIMVIMVim is an advanced text editor that seeks to provide the power of the de-facto Unix editor 'Vi', witt						
Scriptingvulnerability inorvulnerability inorvulnerability inorvulnerability insquidGuard.org/DSQUID-squidGuard.cgi in squidGuard before 1.5 allows remote attackers to inject arbitrary web script or HTML via a blocked site link. REFERENCE: CVE-2015- 8936squidGuard.org/D ownloads/Patc hes/1.4/Readm e.Patch- 20150201SQUID- 280217/3VideoinsightWeb Client The WebClient class provides common methods for sending data to or receiving data from any loo intranet, or Internet resource identified by a URI.NAA-VID-WE C- 280217/3Execute Code; SQL Injection13-02-20177.5An issue was discovered in VideoInsight Web Client Version 6.3.5.11 and previous versions. SQL Injection vulnerability has been identified, which may allow remote code execution. REFERENCE: CVE-2017- S1515NAA-VID-WE C- 280217/3VIMVIMVim is an advanced text editor that seeks to provide the power of the de-facto Unix editor 'Vi', witt	-					
Videoinsight     Web Client     The WebClient class provides common methods for sending data to or receiving data from any lointranet, or Internet resource identified by a URI.     Execute Code;   13-02-2017   7.5   An issue was discovered in VideoInsight Web Client Version 6.3.5.11 and previous versions. SQL Injection vulnerability has been identified, which may allow remote code execution.   AeVID-WE C-280217/3     VIM   VIM     VIM   VIM     Vim is an advanced text editor that seeks to provide the power of the de-facto Unix editor 'Vi', wit		09-02-2017	4.3	vulnerability in squidGuard.cgi in squidGuard before 1.5 allows remote attackers to inject arbitrary web script or HTML via a blocked site link. <b>REFERENCE: CVE-2015-</b>	uidguard.org/D ownloads/Patc hes/1.4/Readm e.Patch-	-
Web Client     The WebClient class provides common methods for sending data to or receiving data from any logintranet, or Internet resource identified by a URI.     Execute Code;   13-02-2017   7.5   An issue was discovered in VideoInsight Web Client Version 6.3.5.11 and previous versions. SQL Injection vulnerability has been identified, which may allow remote code execution.   NA   A-VID-WE C-VIM     VIM   VIM   VIM   VIM   VIM   VIM	Videoinsight			0730		
Execute Code;   13-02-2017   7.5   An issue was discovered in   NA   A-VID-WE     SQL Injection   VideoInsight Web Client   VideoInsight Web Client   C-   280217/3     Previous versions. SQL   Injection vulnerability has   been identified, which   280217/3     Injection.   REFERENCE: CVE-2017-   For the securition.   For the securition.     VIM   Vim is an advanced text editor that seeks to provide the power of the de-facto Unix editor 'Vi', with	Web Client The WebClient cla				or receiving data f	rom any local,
<b>VIM</b> Vim is an advanced text editor that seeks to provide the power of the de-facto Unix editor 'Vi', wit	Execute Code;	13-02-20177.5An issue was discover VideoInsight Web Clic Version 6.3.5.11 and previous versions. SQ Injection vulnerabilit been identified, which may allow remote coor execution.REFERENCE: CVE-20		An issue was discovered in VideoInsight Web Client Version 6.3.5.11 and previous versions. SQL Injection vulnerability has been identified, which may allow remote code execution. <b>REFERENCE: CVE-2017-</b>	NA	A-VID-WEB C- 280217/344
Vim is an advanced text editor that seeks to provide the power of the de-facto Unix editor 'Vi', with	VIM				1 	
	Vim is an advance		hat seeks	s to provide the power of the	e de-facto Unix edi	tor 'Vi', with a

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

Overflow	10-02-2017	7.5	vim before patch 8.0.0322 does not properly validate values for tree length when handling a spell file, which may result in an integer overflow at a memory allocation site and a resultant buffer overflow. <b>REFERENCE: CVE-2017-</b> <b>5953</b>			æ	1 //0				M-VIM- 17/345	
Visonic												
<b>Powerlink2 Firm</b> Visonic's PowerL and control.		st compr	ehensive	e Internet	-based so	olut	tion fo	r advano	ced 1	home	security	
Cross Site Scripting	13-02-2017	4.3	An issue was discovered in Visonic PowerLink2, all versions prior to October 2016 firmware release. User controlled input is not neutralized prior to being placed in web page output (CROSS-SITE SCRIPTING). <b>REFERENCE: CVE-2016-</b> 5811				NA				POWER- 280217/346	
Webkit												
Webkit is a layou	it engine softwa	ire comn	onent fo	r renderij	ng weh ng	ວດອ	s in w	eh hrow	corc			
Denial of Service	03-02-2017	4.3	onent for rendering web page JavaScriptCore in WebKit allows attackers to cause a denial of service (out-of- bounds heap read) via a crafted Javascript file. <b>REFERENCE: CVE-2016-</b> <b>9642</b>			a	NA			A-WEB- WEBKI- 280217/347		
Wordpress			_							•		
Mail Plugin     WP Mail plugin is simply a wp network mail or message system. Users can send mail or messages to other users over one wp network.												
Cross Site Scripting	10-02-2017	4.3	An issue was discovered in the WP Mail plugin before 1.2 for WordPress. The replyto parameter when composing a mail allows				https://cjc.im/a A-WOF dvisories/0006 MAIL - / 28021					
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6		6-7	7-8		8-9	9-10	

			would execut contex receiv	eflected XS allow you e JavaScri t of the us ing the ma <b>RENCE: CV</b>	to pt in the ser nil.				
Xabber									
<b>Xabber</b> Xabber is the mo	ost nonular oner	-source	XMPP cl	ient for Ai	ndroid				
NA	09-02-2017	4.3	An inc impler 0280: in mul allows to imp includ vulner display variou engine CVE is manua 1.0.30 1.0.74		of "XEP- Carbons" P clients attacker any user, ets, in the cation's ows for social cks. This er (only if ed: 1.0.30, 1.0.3 -	,		Х	A-XAB- XABBE- 280217/34
Yaxim									
<i>Bruno;Yaxim</i> Bruno is a Jab source yaxim ap								ion of	f the ope
NA	09-02-2017	4.3	An inc impler 0280: in mul allows to imp includ vulner display variou engine CVE is	orrect nentation Message ( tiple XMP a remote ersonate a ing contac able appli y. This allo s kinds of ering atta for yaxim (0.8.6 - 0.	of "XEP- Carbons" P clients attacker any user, ets, in the cation's ows for social cks. This and	NA		E	A-YAX- 3RUNO- 280217/35
CV Scoring Scale	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9 9-10

			REFEI 5589	RENCE: CV	Æ-2017-				
Zoneminder			3309						
Zoneminder									
	ree onen sourc	re Closed	l-circuit	television	software	applicat	ion devel	oned for	Linux
ZoneMinder is a f Gain Information File Inclusion	ree, open sourc	2.1	A file c inclusi exists web/v ZoneM v1.30. unfilte being j which auther read lo (e.g., / contex user (v attack dot) in within zm/in path=	lisclosure on vulner in inder 1.x 0 because red user-i passed to allows an aticated at ocal system etc/passw ct of the wo www-data vector is a the path	and ability php in through of nput readfile() tacker to n files vd) in the eb server ). The a (dot paramete iew=file&	r	uon devel	A-ZO ZON	DN-
Cross Site Scripting	06-02-2017	4.3	Multip vulner form a param v1.30 a source applica a remo execut within client' is /zm sample includ action gin[XS view= view=	=login&vie	xist withi put oneMinde an open- ver web ch allows er to is scripts nticated . The URL p and ers could ew=postlo SS] S]	r D		A-Z0 Z0N 280	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			[1][cnj]=and[XSS] view=events&filter%5Bte rms%5D%5B1%5D%5Bc nj%5D=and[XSS] view=events&filter%5Bte rms%5D%5B1%5D%5Bc nj%5D=[XSS]and view=events&limit=1%22 %3E%3C/a%3E[XSS] (among others). <b>REFERENCE: CVE-2017-</b> <b>5367</b>		
Cross Site Request Forgery	06-02-2017	6.8	ZoneMinder v1.30 and v1.29, an open-source CCTV server web application, is vulnerable to CSRF (Cross Site Request Forgery) which allows a remote attack to make changes to the web application as the current logged in victim. If the victim visits a malicious web page, the attacker can silently and automatically create a new admin user within the web application for remote persistence and further attacks. The URL is /zm/index.php and sample parameters could include action=user uid=0 newUser[Username]=atta cker1 newUser[Password]=Pass word1234 conf_password=Password 1234 newUser[System]=Edit (among others). <b>REFERENCE: CVE-2017- 5368</b>	NA	A-ZON- ZONEM- 280217/353

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

# **Application; Operating System (A/OS)**

## **Canonical; Debian/ Exim**

#### Ubuntu Linux/Debian Linux/Exim

Ubuntu is a computer operating system based on the Debian Linux distribution and distributed as free and open source software, using its own desktop environment/ Debian is an operating system and a distribution of Free Software/ Exim is a mail transfer agent (MTA) used on Unix-like operating systems.

NA	01-02-2017	2.6	Exim before 4.87.1 might	https://bugs.exi	A-OS-CAN-
			allow remote attackers to	m.org/show_bu	UBUNT-
			obtain the private DKIM	g.cgi?id=1996	280217/354
			signing key via vectors		
			related to log files and		
			bounce messages.		
			<b>REFERENCE: CVE-2016-</b>		
			9963		
Dobian: Fodora	project /Incher	Drojoct	•	·	

#### Debian; Fedoraproject/Jasper Project

#### Debian Linux/Fedora/Jasper

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project/ Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/ Jasper is an open source platform for developing always-on, voice-controlled applications.

Denial of Service	15-02-2017	4.3	The jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.4 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted YRsiz value in a BMP image to the imginfo command. <b>REFERENCE: CVE-2016-</b> <b>8692</b>	https://bugzilla .redhat.com/sh ow_bug.cgi?id= 1385502	A-OS-DEB- DEBIA- 280217/355
Denial of Service	15-02-2017	4.3	The jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.4 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted XRsiz value in a	https://bugzilla .redhat.com/sh ow_bug.cgi?id= 1385502	A-OS-DEB- DEBIA- 280217/356

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

	BMP image to the imginfo command.	
	REFERENCE: CVE-2016- 8691	

## Debian;Novell;Opensuse Project;Suse/Graphicsmagick;Suse

Scale

Debian Linux / Leap / Opensuse / Linux Enterprise Software Development Kit / Graphicsmagick / Linux Enterprise Debuginfo; Studio Onsite

Debian is an operating system and a distribution of Free Software/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system/ openSUSE, formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies/ SUSE Linux Enterprise Software Development Kit 11 is a comprehensive development tool kit that is designed to support developers, as well as independent hardware vendors (IHVs) and independent software vendors (ISVs), in creating applications on or porting them to SUSE Linux Enterprise 11 products/ GraphicsMagick is the swiss army knife of image processing - comprised of 267K physical lines (according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF/ NA : SUSE Studio Onsite is a Web application for building and testing appliances in a Web browser.

				incation for building and testing appliances in a web browser.							
Denial of	0	3-02-2017	4.3	Graphi	csMagick	1.3.23	-	s://bugzil		A-OS-D	EB-
Service				allows	remote at	tackers t		nat.com/s		DEBIA-	
				cause a	a denial of	service		oug.cgi?id	= 2	280217	7/357
				(NULL	pointer		1306	5148			
				derefe	rence) via	a crafted					
				SVG fil	e, related t	to the (1)					
				Drawl	mage func	tion in					
				magicl	x/render.c	, (2)					
				SVGSta	rtElemen	t function	1				
				in code	ers/svg.c, a	and (3)					
				TraceA	rcPath fu	nction in					
				magicl	x/render.c	•					
				REFEF	<b>ENCE: CV</b>	E-2016-					
				2318							
Denial of	0	3-02-2017	4.3	-		http	s://bugzil	lla /	A-OS-D	EB-	
Service;				in GraphicsMagick 1.3.23		.redl	nat.com/s	h l	DEBIA-		
Overflow				allow remote attackers to		ow_l	oug.cgi?id	= 2	280217	7/358	
				cause a denial of service		1300	6148				
				(crash) via a crafted SVG							
				file, related to the (1)							
				TracePoint function in							
				magick/render.c, (2)							
				GetToken function in							
				magicl	x/utility.c,	and (3)					
				-	insformTo						
				functio	on in codei	s/svg.c.					
CV				3-4 4-5 5-6							

				RENCE: CV	/E-2016-						
			2317								
			_	_							
Debian;Novell;O		· ·		0							
Debian Linux/Le											
Debian is an oper	rating system a	nd a dist	ributio	n of Free	Software	/ LE	EAP is	s an onlir	ne c	ommu	nity for
energy analysts	working for su	stainabil	ity and	the home	e of the L	LEAI	P sof	tware sys	sten	n/ ope	enSUSE,
formerly SUSE Lin	nux and SuSE L	inux Pro	fessiona	l, is a Linu	ux-based	pro	ject a	nd distri	buti	on spo	nsored
by SUSE Linux	GmbH and oth	ner comp	oanies/	Graphics	Magick is	s th	ie sw	viss army	/ ki	nife of	image
processing - com	<b>•</b>		~	0						-	
code in the base			-				-				
collection of tools				0	0		-	-		0	
major formats inc		int forma				G-20	)00, P	'NG, PDF,	PN	M, and	TIFF.
Denial of	06-02-2017	5	_	r underflo			-	://sourc		A-OS-	
Service;			<b>^</b>	BIM funct			0	net/p/gr		DEBL	
Overflow				/meta.c iı			-	magick/		2802	17/359
			-	csMagick				/5c7b6d			
				rlier allov				25e99c5			
				ers to cau				343914e	bf		
				ice (appli		d821	3ef/				
				via a craf							
				which tri							
			heap-based buffer								
			overflo								
				RENCE: CV	/E-2016-						
			7800								
Debian; Novell/											
Debian Linux/Le											
Debian is an ope											
(MTA) used on											
working for susta							-		Col	or Eng	ine is a
free, open source											
Denial of	03-02-2017	5.8		pe_MLU_			-	://githul		A-OS-	
Service; Gain				on in cmst			om/r	nm2/Litt	le	DEBI	
Information				CMS (aka l			-			2802	17/360
				remote a			'	/commit/			
				sensitive				a7bc18b			
				ation or c				21d815d			
				of service				8e20458	1		
			U	with a cra			e2				
			<b>^</b>	, which tr	00						
				bounds h	-						
				RENCE: CV	/E-2016-						
Debian; Opensus	se Proiect / Gr	anhicsm	10165 1 agick	, 							
		apinesii									
CV 0-1	1-2	2-3	3-4	4-5	5-6	e	6-7	7-8	8	8-9	9-10
Scoring Scale											

## Debian Linux / Opensuse / Graphicsmagick

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project / openSUSE, formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies / GraphicsMagick is the swiss army knife of image processing - comprised of 267K physical lines (according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF.

Overflow	15-02-2017	6.8	The MagickMalloc function in magick/memory.c in GraphicsMagick 1.3.25 allows remote attackers to	https://bugzilla .redhat.com/sh ow_bug.cgi?id= 1385583	A-OS-DEB- DEBIA- 280217/362
			have unspecified impact via a crafted image, which triggers a memory allocation failure and a "file truncation error for corrupt file." <b>REFERENCE: CVE-2016-</b> <b>8684</b>	100000	
Overflow	15-02-2017	6.8	The ReadPCXImage function in coders/pcx.c in GraphicsMagick 1.3.25 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure and a "file truncation error for corrupt file." <b>REFERENCE: CVE-2016-</b> <b>8683</b>	http://hg.code.s f.net/p/graphic smagick/code/r ev/b9edafd479 b9	A-OS-DEB- DEBIA- 280217/363

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

# Debian Linux/Opensuse/Imagemagick

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project / openSUSE, formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies / ImageMagick is a software suite to create, edit, compose, or convert bitmap images.

Overflow	15-02-2017	6.8	The	https://github.c	A-OS-DEB-
			AcquireQuantumPixels	om/ImageMagi	DEBIA-
			function in	ck/ImageMagic	280217/364
			MagickCore/quantum.c in	k/issues/268	
			ImageMagick before 7.0.3-		
			1 allows remote attackers		
			to have unspecified impact		
			via a crafted image file,		
			which triggers a memory		
			allocation failure.		
			<b>REFERENCE: CVE-2016-</b>		
			8677		

#### Debian/Dicom

## Debian Linux/Dcmtk

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project / DCMTK is a collection of libraries and applications implementing large parts the DICOM standard

210011000000					
Denial of	15-02-2017	5	Stack-based buffer	https://bugzilla	A-OS-DEB-
Service;			overflow in the	.redhat.com/sh	DEBIA-
Overflow			parsePresentationContext	ow_bug.cgi?id=	280217/365
			function in storescp in	1405919	
			DICOM dcmtk-3.6.0 and		
			earlier allows remote		
			attackers to cause a denial		
			of service (segmentation		
			fault) via a long string sent		
			to TCP port 4242.		
			<b>REFERENCE: CVE-2015-</b>		
			8979		

#### Debian / Graphicsmagick

# Debian Linux / Graphicsmagick

Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project / GraphicsMagick is the swiss army knife of image processing- comprised of 267K physical lines (according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF.

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

Overflow	15-02-2017	6.8	The AcquireMagickMemory function in MagickCore/memory.c in GraphicsMagick before 7.0.3.3 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure. <b>REFERENCE: CVE-2016-</b> 8862		uireMagickMemory.redhction inow_bgickCore/memory.c in1387phicsMagick before13873.3 allows remoteaackers to haveapecified impact via afted image, whichgers a memorycation failure.FERENCE: CVE-2016-a		.redhat.com/sh ow_bug.cgi?id= 1387135		A-OS-DEB- DEBIA- 280217/366		
Debian/Libtiff											
<b>Debian Linux/Libtiff</b> Debian is a Unix-like computer operating system that is composed entirely of free software, most of which is under the GNU General Public License and packaged by a group of individuals participating in the Debian Project / Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files.											
Denial of Service; Overflow	06-02-2017	4.3	writeB ps fund LibTIF allows cause a (out-of crafted	r overflow ufferToSe ction in tif F before 4 remote at a denial of f-bounds r l tif file. <b>EENCE: CV</b>	parateStr fcrop.c in .0.7 tackers to service read) via a	i .red ow_ 139	s://bugzill hat.com/sl bug.cgi?id= 7726	n   I	A-OS-DEB- DEBIA- 280217/367		
Fedoraproject;N	lovell;Opensu	se Projec	t;Suse/	Libgit2 P	roject						
Fedoraproject;Novell;Opensuse Project;Suse/Libgit2 ProjectFedora/Leap/Leap;Opensuse/Linux Enterprise/Libgit2Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system; OpenSUSE, formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies/ SUSE Linux Enterprise Desktop delivers essential office functionality affordably, and was built to coexist with other operating systems/ libgit2 is a portable, pure C implementation of the Git core methods provided as a re-entrant linkable library with a solid API, allowing you to write native speed custom Git applications in any language which supports C bindings.											
Denial of Service	03-02-2017	4.3	The git_oid_nfmt function in commit.c in libgit2 before 0.24.3 allows remote attackers to cause a denial of service (NULL			.red ow_	s://bugzill hat.com/sl bug.cgi?id= 3211	n   I	A-OS-FED- FEDOR- 280217/368		
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-1	9 9-10		

			pointer dereference) via a cat-file command with a crafted object file. <b>REFERENCE: CVE-2016-</b> <b>8569</b>							
Denial of Service	03-02-2017	4.3	The git_commit_message function in oid.c in libgit2 before 0.24.3 allows remote attackers to cause a denial of service (out-of- bounds read) via a cat-file command with a crafted object file. <b>REFERENCE: CVE-2016- 8568</b>	https://bugzilla .redhat.com/sh ow_bug.cgi?id= 1383211	A-OS-FED- FEDOR- 280217/369					
Fedoraproject;C	) pensuse Proje	ect/Jaspe	er Project	•						
Fedoraproject;Opensuse Project/Jasper ProjectFedora/Opensuse/JasperFedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/ openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies/Jasper is an open source platform for developing always-on, voice-controlled										

applications.	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	1		0 , ,	
Denial of Service; Execute Code	15-02-2017	6.8	Double free vulnerability in the mem_close function in jas_stream.c in JasPer before 1.900.10 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted BMP image to the imginfo command. <b>REFERENCE: CVE-2016-</b>	https://bugzilla .redhat.com/sh ow_bug.cgi?id= 1385507	A-OS-FED- FEDOR- 280217/370
			8693		

## Fedoraproject/Jasper Project

#### Fedora/Jasper

Scale

Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat /Jasper is an open source platform for developing always-on, voice-controlled applications.

					entromo.					
Denial of		15-02-2017	4.3	The br	The bmp_getdata function https://bugzilla					OS-FED-
Service				in	in .redhat.com/sh					DOR-
				libjasp	, , , , , , , , , , , , , , , , , , , ,				= 28	0217/371
				in JasP	in JasPer before 1.900.5 1385499					
				allows	allows remote attackers to					
				cause a	cause a denial of service					
CV										
Scoring	0-1	1-2	2-3	3-4	<b>4-5</b>	5-6	6-7	7-8	8-9	9-10
Sconing										

		_	derefe BMP in comm	pointer rence) via nage in an and. <b>RENCE: CV</b>	i imginfo					
Fedoraproject/I Fedora/Libwebp	,					<u> </u>				
Fedora (formerly community-supp	,	-	0	5					-	5
library and suppo						<sup>o</sup> format			-	
Overflow	03-02-2017	7.5	in libw attack unspe unkno	le integer rebp allow ers to have cified impa wn vector <b>RENCE: CV</b>	rs e act via s.	.redl ow_l	s://bugzi nat.com/s oug.cgi?id 9338	sh	FEDC	-FED- )R- 17/372
Fedoraproject/0	Openjpeg		<u> </u>							
Fedora/Openjpeg     Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/OpenJPEG is an open-source library to encode and decode JPEG 2000 images.										
Denial of	03-02-2017	4.3		-by-zero		http	s://bugzi	lla	A-OS-	-FED-
Service			vulner opj_tco tcd.c in 2.1.1 a attacko of serv crash) file. N exists incorr REFEF 7947. <b>REFEF</b> 4 <b>797</b>	ability in t l_init_tile f n OpenJPE llows rem ers to cause rice (applie via a craft OTE: this i because of ect fix for ENCE: CV	function i G before ote se a denia cation ced jp2 issue f an E-2014- <b>TE-2016-</b>	.redl n ow_1 133! l	nat.com/s oug.cgi?id 5483	sh  =	FEDC 2802	0R- 17/373
Denial of Service; Overflow	03-02-2017	4.3	overflo color_o comm OpenJ allows	w in the .redhat.com/sh F				FEDC	-FED- )R- 17/374	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

			(crash file.	) via a crat	fted .j2k					
			-	RENCE: CV	E-2016-					
Fedoraproject/	Suckless									
Fedora/Slock Fedora (formerly community-supp is the simplest X	y Fedora Core) oorted Fedora P	-	-	-					-	-
Bypass	15-02-2017	5	bypass vector invalic which pointe crash.	illows atta s the scree s involving l password triggers a r derefere RENCE: CV	n lock via g an l hash, NULL nce and	ess.o omm ec0fe 78cb	//git.sucl rg/slock/ nit/?id=d8 5fdc8a24 488a006 946fcb29	/c 3b 6d	A-OS- FEDO 2802	
IBM/IBM										
Security Access A Access Manager IBM Security Actechnologies and Gain Information	<b>For Web 8.0 Fi</b> cess Manager e	i <b>rmware</b> enables l	/Securi ousiness ianagem IBM Se Manag allow a obtain inform failure HTTP Securi exploit to obta inform the mi	ty Access and the second secon	Manager : re securel nployees a cess b could ttacker to sed by the ly enable sport cker could erability ve ag man in niques.	For Mor y adop nd cons http: m.co /doc id=sv 6	<b>bile</b> t web, m	b ort ?u	e, and A-OS- SECU	l cloud IBM-
Bypass	07-02-2017	4.3	S043Http://www.ibIBM Security Accesshttp://www.ibManager for Web 7.0.0,m.com/support8.0.0, and 9.0.0 could/docview.wss?uallow a remote attacker toid=swg2199682bypass security6restrictions, caused byimproper contentvalidation. By persuading				rt ?u	A-OS- SECU 2802		
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

CV Scoring Scale	0-1 1-2	2.	-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10
software syste Denial of Service			ł.3	The milibarch keep tr when e ahead, remote a denia via a cr trigger	nterface for reading/writing analysts working for sustaina The mtree bidder in libarchive 3.2.1 does not keep track of line sizes when extending the read- ahead, which allows remote attackers to cause a denial of service (crash) via a crafted file, which triggers an invalid read in the (1) detect_form or (2)			https://github.c om/libarchive/l ibarchive/com mit/eec077f52b fa2d3f7103b4b 74d52572ba8a 15aca			
	e library prov	vides a	-				-	-			
Gain Information SQL Injection	08-02-2		2.1	crafted attacke vulner validat with m <b>REFEF</b> <b>3020</b> The IB Manag include files th obfusc passwe auther access <b>REFEF</b> <b>5013</b> IBM Se Manag vulner injection attacke special statem allow t inform	n to open l content, a er could es ability to h cion and lo alicious co <b>RENCE: CV</b> M Security er applian es configu at contain ated plain ords which ticated us <b>RENCE: CV</b> ecurity Acc er for Wel able to SQ on. A remo er could se lly-crafted tents which tabase. <b>RENCE: CV</b>	an sploit this bypass ad a page ontent. <b>F-2016-</b> <b>F-2016-</b> <b>F-2016-</b> <b>F-2016-</b> <b>F-2015-</b> <b>T-2015-</b> <b>Cess</b> b is L b te end SQL h could er to view he back-	s http m.c /do id=s 2 http m.c /do id=s 7	o://www.i om/suppo cview.wss swg21993 o://www.i om/suppo cview.wss swg21995	b b rt ?u	A-OS- SECU	R- 17/378 -IBM-

	bid_entry function in libarchive/archive_read_s upport_format_mtree.c. <b>REFERENCE: CVE-2016-</b>	
	8688	

#### Moxa/Moxa

Scale

Nport 5100 Series Firmware;Nport 5100a Series Firmware;Nport 5200 Series Firmware;Nport 5200a Series Firmware;Nport 5400 Series Firmware;Nport 5600 Series Firmware;Nport 5x50a1m12 Series Firmware;Nport 6100 Series Firmware;Nport P5150a Series Firmware/Nport 5600-8dtl Series Firmware

The MOXA NPort 5000 and 6000 Series device allows a Serial GSM modem to be connected to a Swivel appliance through an ethernet network connection. Since 2002, Moxa has continued to grow at a rate of about 30% each year. A branch office has been opened in Europe, and Moxa's product offerings have expanded to include managed industrial Ethernet switches, embedded computers, and industrial wireless solutions.

WII CIESS 301							1			
NA	1	3-02-2017	7.8		ue was dis					S-MOX-
					NPort 511		IS			ORT-
				-	o 2.6, NPo				280	217/381
				5130/	5150 Serie	es				
					ns prior to					
				NPort	5200 Serie	es				
				versio	ns prior to	2.8,				
				NPort	5400 Serie	es				
				versio	ns prior to	3.11,				
				NPort	5600 Serie	es				
				versio	ns prior to	3.7,				
				NPort	5100A Ser	ies &				
				NPort	P5150A ve	ersions				
				prior t	o 1.3, NPo	rt 5200A				
				Series	versions p	orior to				
				1.3, NF	ort 5150Å	AI-M12				
				Series	versions p	orior to				
				1.2, NF	ort 5250 <sup>7</sup>	AI-M12				
				Series	versions p	orior to				
					ort 5450 <sup>7</sup>					
				Series	versions p	orior to				
				1.2, NF	ort 5600-	8-DT				
				Series	versions p	orior to				
					ort 5600-					
					versions p					
					ort 6x50 S					
					ns prior to					
					IA5450A v					
				prior to v1.4. The amount						
				of resources requested by						
CV										
Scoring	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

	1			I	,						
			a malicious actor is not								
			restricted, leading to a								
			denial-of-service caused								
			by resource exhaustion.								
			<b>REFERENCE: CVE-2016-</b>								
			9367								
Artifex / Fedora	project										
<i>Mujs / Fedora</i> MuJS is a lightweight Javascript interpreter designed for embedding in other software to extend them with scripting capabilities/ Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project.											
Denial of	03-02-2017	5	Integer overflow in the	https://hugzilla	A-OS-ART-						
Service;	03-02-2017	Э	0	https://bugzilla .redhat.com/sh	MUJS/-						
Overflow			js_regcomp function in regexp.c in Artifex	ow_bug.cgi?id=	280217/382						
Overnow			Software, Inc. MuJS before	1390266	200217/302						
			commit	1390200							
			b6de34ac6d8bb7dd5461c								
			57940acfbd3ee7fd93e								
			allows attackers to cause a								
			denial of service								
			(application crash) via a								
			crafted regular expression.								
			<b>REFERENCE: CVE-2016-</b>								
			9108								
Dlitz/Fedorapro	oiect										
Pycrypto/Fedora	·										
		ovides	secure hash functions and	various encryption	n algorithms/						
	• · · •		erating system based on the		<b>U</b> ,						
		P			eloped by the						
community-suppo	orted Fedora P	roiect.		LINUX Kerner, dev	eloped by the						
<i>v</i>	orted Fedora P 15-02-2017	· · ·	Heap-based buffer	1							
Execute Code;	<mark>orted Fedora P</mark> 15-02-2017	roject. 7.5	Heap-based buffer overflow in the ALGnew	https://github.c	A-OS-DLI-						
<i>v</i>		· · ·	overflow in the ALGnew	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code;		· · ·	overflow in the ALGnew function in	https://github.c	A-OS-DLI-						
Execute Code;		· · ·	overflow in the ALGnew function in block_templace.c in	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code;		· · ·	overflow in the ALGnew function in block_templace.c in Python Cryptography	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code;		· · ·	overflow in the ALGnew function in block_templace.c in	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code;		· · ·	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto)	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code;		· · ·	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code;		· · ·	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code;		· · ·	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code;		· · ·	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code;		· · ·	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py.	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code;	15-02-2017	7.5	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py. <b>REFERENCE: CVE-2013-</b> 7459	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code; Overflow	15-02-2017 /Novell;Opens	7.5 suse Pro	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py. <b>REFERENCE: CVE-2013-</b> 7459	https://github.c om/dlitz/pycry	A-OS-DLI- PYCRY-						
Execute Code; Overflow Graphicsmagick	15-02-2017 :/Novell;Opensu	7.5 suse Pro	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py. <b>REFERENCE: CVE-2013-</b> 7459	https://github.c om/dlitz/pycry pto/issues/176	A-OS-DLI- PYCRY- 280217/383						
Execute Code; Overflow Graphicsmagick Graphicsmagick, GraphicsMagick i	15-02-2017 <b>/Novell;Opens</b> /Leap/Opensu is the swiss a	7.5 suse Pro	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py. <b>REFERENCE: CVE-2013-</b> 7459 Dject	https://github.c om/dlitz/pycry pto/issues/176	A-OS-DLI- PYCRY- 280217/383 physical lines						
Execute Code; Overflow Graphicsmagick Graphicsmagick, GraphicsMagick i	15-02-2017 <b>/Novell;Opens</b> /Leap/Opensu is the swiss a	7.5 suse Pro	overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py. <b>REFERENCE: CVE-2013-</b> 7459	https://github.c om/dlitz/pycry pto/issues/176	A-OS-DLI- PYCRY- 280217/383						

(according to David A. Wheeler's SLOCCount) of source code in the base package (or 1,225K including 3rd party libraries) it provides a robust and efficient collection of tools and libraries which support reading, writing, and manipulating an image in over 88 major formats including important formats like DPX, GIF, JPEG, JPEG-2000, PNG, PDF, PNM, and TIFF/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system / openSUSE formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies/

	id other compani									
Denial of Service	03-02-2017	4.3	Graphi 1.3.24 attacke of serv except crash) file.	k/render.c icsMagick allows rer ers to caus rice (arithr ion and ap via a craft RENCE: CV	before note se a denia netic oplication ced svg	.red ow_ ll 133	os://bugzi hat.com/s bug.cgi?ic 3410	sh	GRAF	-GRA- PH- 17/384
Denial of Service	06-02-2017	5	in code Graphi allows cause a (out-o via a fi "unter	FFGetField ers/tiff.c in icsMagick remote at a denial of f-bounds h le contain minated" s RENCE: CV	n 1.3.24 tackers t service neap read ing an string.	.red ow_ o 137	s://bugzi hat.com/s bug.cgi?ic 4233	sh	GRAF	-GRA- PH- 17/385
Overflow	06-02-2017	7.5	overflo Escape functio Graphi 1.3.25 attacko unspec unkno	based buff ow in the Parenthes on in icsMagick allows rer ers to have cified impa wn vector <b>RENCE: CV</b>	.red ow_	s://bugzi hat.com/s bug.cgi?ic 4233	sh	GRAF	-GRA- PH- 17/386	
Overflow	06-02-2017	7.5	MVG a code in 1.3.24 attacke unspee	overflow i nd SVG ren n Graphics allows ren ers to have cified impa wn vector	.red ow_	https://bugzilla .redhat.com/sh ow_bug.cgi?id= 1374233			A-OS-GRA- GRAPH- 280217/387	
CV 0	-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	3-9	9-10

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

Denial of Service Libarchive/Oper Libarchive/Leap		7.8	patch for CVE-2016-2317. <b>REFERENCE: CVE-2016-</b> <b>7446</b> The Utah RLE reader in GraphicsMagick before 1.3.25 allows remote attackers to cause a denial of service (CPU consumption or large memory allocations) via vectors involving the header information and the file size. <b>REFERENCE: CVE-2016-</b> <b>7448</b>				edha	//bugzi at.com/s 1g.cgi?id 233	sh	GRAI	-GRA- 2H- 217/388
The libarchive lib LEAP is an online software system.	orary provides	-				-		-			
Denial of Service	15-02-2017	5	in archiv mat_7: 3.2.1 a attacke of serv read) Empty a head	The read_Header function			https://bugzilla .redhat.com/sh ow_bug.cgi?id= 1377925			A-OS LIBA 2802	
Denial of Service; Overflow	15-02-2017	5	Stack-l overflo safe_fp tar/uti 3.2.1 a attacko of serv non-pr charac	8689 Stack-based buffer overflow in the safe_fprintf function in tar/util.c in libarchive 3.2.1 allows remote attackers to cause a denial of service via a crafted non-printable multibyte character in a filename. REFERENCE: CVE-2016-			edha	//bugzi at.com/s ug.cgi?id 926	sh	LIBA	-LIB- R- 17/390
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8	8-9	9-10

		Applic	ation; Hardware	(A/H)								
F5/F5												
Big-ip Access Policy Manager; Big-ip Advanced Firewall Manager; Big-ip Analytics; Big-ip												
Application Acce	eleration Man	ager; Bi	g-ip Application Se	ecurity M	lanager; Big-ip (	Global Traffic						
			g-ip Local Traffic	Manage	er; Big-ip Policy	Enforcement						
Manager/Big-ip BIG-IP System -			d hardware gives y	ou the a	hility to control t	he traffic that						
passes through ye		ware an	a naraware gives y	ou the u	binty to control t							
Gain	09-02-2017	5	A BIG-IP virtual ser	ver	https://support	A-H-F5/-						
Information			configured with a C		.f5.com/csp/art	BIG-I-						
			SSL profile that has non-default Sessior		icle/K0512167 5	280217/391						
			Tickets option enal		5							
			may leak up to 31 b									
			uninitialized memo	•								
			remote attacker ma	•								
			exploit this vulnera to obtain Secure So									
			Layer (SSL) session									
			from other sessions									
			possible that other	data								
			from uninitialized	•								
			memory may be read	turnea								
			REFERENCE: CVE-	2016-								
			9244									
			Hardware (H)									
Cisco												
Industrial Ether												
		-	000) Series Switches		l the proven C	isco Catalyst						
technologies prev Denial of	03-02-2017	rise netw	<mark>vorks to industrial ne</mark> A vulnerability in tl		https://tools.cis	H-CIS-						
Service; Gain	03-02-2017	/.1	implementation of		co.com/security	INDUS-						
Information			Common Industrial		/center/content	280217/392						
			Protocol (CIP)		/CiscoSecurityA							
			functionality in Cis		dvisory/cisco-							
			Industrial Ethernet Series Switches cou		sa-20170201- psc1							
			allow an unauthent		pser							
			remote attacker to									
CV				-								
Scoring 0-1	1-2	2-3	3-4 4-5	5-6	6-7 7-8	8-9 9-10						
Scale												

INA		.3-02-201/	2.1	Moxa NPort 5110 versions NP						
5200a Set 5x50a1-m Nport 560 The MOXA appliance to of about 3	0 Series ries Firn 12 Serie 0-8-dtl S NPort 50 hrough a 0% each ided to in lutions.	Firmware; nware; Np es Firmwan eries Firmw 000 and 600 an ethernet year. A br	Nport 5 ort 540 re; Nport vare 00 Series network anch offi	100a Series 0 Series t 6100 S devices a connecti ce has be istrial Et	Firmwar Series Fir allow a Ser ion. Since 2 een opene hernet swi	vare; Nport e; Nport mware;N ial GSM r 2002, Mo d in Euro itches, em	ort 5200 t 5600 Iport P: nodem t xa has c ope, and ibedded	0 Series Fir Series Fir 5150a Seri o be connec ontinued to Moxa's pro computers	nware es Firi ted to a grow a oduct o , and in	; Nport mware/ a Swivel at a rate offerings
				hardco 'core' i allows unauth access <b>REFEF</b> 8491	oded accou in Fortinet attackers norized rea via a remo <b>RENCE: CV</b>	nt named FortiWL to gain ad/write ote shell. <b>E-2016-</b>	l rd.co C y/FG	om/advisor -IR-16-065	FOR	
devices to	support l demands		, high pe	rformano tivity.		dictability	y while a	ess access po addressing r s://fortigua	nission	-critical
				memo Inform Known 15.2(5 Fixed I 15.2(5	ion due to ry leak. Mo nation: CSC n Affected .4.32i)E2. Releases: .4.62i)E2. <b>RENCE: CV</b>	ore Svc54788 Releases: Known				

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

Cross Site Scripting	13-02-2017	4.3	versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. A configuration file contains parameters that represent passwords in plaintext. <b>REFERENCE: CVE-2016-</b> 9348 An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 3.6, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort 5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.2, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to	NA	H-OS-MOX- NPORT- 280217/395
-------------------------	------------	-----	---	----	-----------------------------------

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

			2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. User- controlled input is not neutralized before being output to web page (CROSS-SITE SCRIPTING). <b>REFERENCE: CVE-2016-</b> 9371		
Bypass	13-02-2017	5	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. An attacker can freely use brute force to determine parameters	NA	H-OS-MOX- NPORT- 280217/396

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

			authen	l to bypas itication. RENCE: CV					
Cross Site Request Forgery	13-02-2017	6.8	An issu Moxa M prior to 5130/3 version NPort version NPort version NPort version NPort prior to Series 1.2, NF Series 1.2, NF Series 1.2, NF Series 2.4, NF Series 2.4, NF version NPort Series 2.4, NF	ae was dis NPort 511 o 2.6, NPo 5150 Serie as prior to 5200 Serie as prior to 5400 Serie as prior to 5400 Serie as prior to 5100A Serie prior to 500 versions prior to 105450A Serie prior to 105450A Serie cont 100 versions prior to 105450A Serie prior to 100 versions prior to 105450A Serie prior to 100 versions prior to 105450A Serie serie to be onally sub oper user EQUEST F SENCE: CV	0 version ort es o 3.6, es o 2.8, es o 3.11, es o 3.7, ries & ersions ort 5200A orior to AI-M12 orior to AI-M12 orior to AI-M12 orior to AI-M12 orior to Series o 1.13.11, versions equests ar e omitted by (CROSS- FORGERY)	e y		NP	DS-MOX- ORT- D217/397
Execute Code; Overflow	13-02-2017	7.5	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series					NP	DS-MOX- ORT- D217/398
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
NA	13-02-2017	7.5	Moxa M prior to 5130/3 version NPort 3 version NPort 3 version NPort 3 NPort 3 prior to Series	NPort 511 o 2.6, NPo 5150 Serie ns prior to 5200 Serie ns prior to 5400 Serie ns prior to 5600 Serie 5100A Serie 5	es ) 3.6, es ) 2.8, es ) 3.11, es ) 3.7, ries & ersions ort 5200A prior to	5		NPC 280	PS-MOX- DRT- 9217/399
			NPort i version NPort i version NPort i NPort i Prior to Series i 1.3, NP Series i 1.2, NP Series i 1.2, NP Series i 2.4, NP Series i 2.4, NP version NPort i prior to overflo may all unauth to rem arbitra	ns prior to 5400 Seri- ns prior to 5600 Seri- ns prior to 5100A Seri- ns prior to 5100A Seri- port 5150A v. o 1.3, NPo versions p Port 5150A versions p Port 5450A versions p Port 5600- versions p Po	es ) 3.11, es ) 3.7, ries & ersions ort 5200A orior to AI-M12 orior to AI-M12 orior to AI-M12 orior to AI-M12 orior to AI-M12 orior to Sentes ) 1.13.11, versions offer ability attacker cute				

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

			1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. Administration passwords can be retried without authenticating. <b>REFERENCE: CVE-2016- 9361</b>		
Execute Code	13-02-2017	10	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort 5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series	NA	H-OS-MOX- NPORT- 280217/400

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

			NPort prior t can be	ns prior to IA5450A o v1.4. Fin updated o rk withou	versions rmware over the				
			allow i execut	ntication, w remote co- ion. <b>RENCE: CV</b>	de	У			
			8369 REFER	CENCE: CV	E-2010-				
		0	perating	g Systen	1 (OS)				
Adcon Telemetr	-								
A850 Telemetry									
The A850 Teleme				•	-	2		-	•
network, a UHF i how to retrieve d			bination	or both -	it is the I	1050 ([	at knows	exactly	when and
Cross Site Scripting	13-02-2017	4.3		ue was dis Telemetr		n NA		0-	-ADC-A850
8				etry Gatev	•			28	30217/401
			Statior	n. The Wel	o Interfac	e			-
				ot neutral					
				ectly neut					
				ontrollabl	-				
				it is place ; this coul					
			-	ss-site scr					
				RENCE: CV					
			2274		0 _ 0				
Binom3			-			1		ł	
<b>Universal Multif</b>	functional Elec	tric Pow	ver Quali	ity Meter	Firmwar	е			
NA			Ĩ	-					
Execute Code;	13-02-2017	4.3		ue was dis		n NA		0.	-BIN-
Cross Site				13 Univers					NIVE-
Scripting				unctional				28	30217/402
				Quality M					
				sent from ous client					
				rly verified					
				. An attacl	-				
				e arbitrar					
				n another					
				er session	•				
				CRIPTING	-				
			REFEF	RENCE: CV	/E-2017-				
CV	10		2.4	4 5	5-6	67	7 9	8.0	9_10

			5164						
Gain Privileges; Gain Information	13-02-2017	5	An issue w BINOM3 U Multifuncti Power Qua INFORMAT flaw can be privileged device. <b>REFERENO</b> 5166	niversal ional Electr llity Meter. FION EXPO e used to ga access to tl	ric An SURE ain he	NA		0-B UNI 280	
Cross Site Request Forgery	13-02-2017	6.8	An issue w BINOM3 U Multifuncti Power Qua There is no generated and/or per function. Si exploitatio vulnerabili silent exect unauthoriz the device configurati changes, an modified co <b>REFERENO</b> 5165	niversal ional Electri lity Meter. o CSRF Tok per page c (sensitive uccessful n of this ity can allow ution of ced actions such as ion parame nd saving onfiguratio	ric en e) w on eter on.	NA		0-B UNI 280	
NA	13-02-2017	7.5	An issue w BINOM3 U Multifuncti Power Qua Users do n option to c own passw <b>REFEREN</b> 5167	niversal ional Electu lity Meter. ot have any hange thei vords.	ric y r	NA		0-B UNI 280	
NA	13-02-2017	10	An issue w BINOM3 U Multifuncti Power Qua of authenti remote ser access to a	niversal ional Electr llity Meter. cation for vice gives	ric Lack	NA		0-B UNI 280	
CV 0-1 Scoring Scale	1-2	2-3	3-4 4	-5 5-	-6	6-7	7-8	8-9	9-10

				configura RENCE: CV					
Carlosgavazzi								1	
Vmu-c Em Firm VMUC EM- the PhotoVoltaic Mo	WebServer Solu	ution for		ergy mar	nagement	applica	tions; VN	AUC PV-	for the
Gain Information	13-02-2017	5	Carlo ( prior t A11_U prior t A17. So is store	ie was dis Gavazzi VN o firmwar 05, and VI o firmwar ensitive in ed in clear <b>RENCE: CV</b>	MU-C EM re Version MU-C PV re Version formation r-text.			VM	AR- U-C- 0217/407
Cross Site Request Forgery	13-02-2017	7.5	Carlo ( prior t A11_U prior t A17. Si exploit SITE R (CSRF) allow e unauth the dev configu change modifi	te was dis Gavazzi VN o firmwar 05, and VI o firmwar uccessful cation of the EQUEST F vulnerable execution torized ac vice such a uration pates, and save ed configue ENCE: CV	AU-C EM re Version MU-C PV re Version his CROSS FORGERY fility can of tions on as trameter ving tration.			VM	AR- U-C- 0217/408
NA	13-02-2017	7.5	An issu Carlo ( prior t A11_U prior t A17. T flaw al applica withou	te was dis Gavazzi VN o firmwar 05, and VI o firmwar he access lows acce ation func at authent <b>RENCE: CV</b>	MU-C EM Te Version MU-C PV Te Version control ss to mos tions ication.			VM	AR- U-C- 0217/409
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Cisco									
Ios Xe									
Cisco IOS XE sof	•				0	tly enh	ances soft	ware	quality and
performance by						1	( () 1	· 0	
Denial of Service; Overflow	03-02-2017	5.4	A vuln handli Cisco o Conver Router unauth attacke device in a de condit Conver Router vulner Cisco I More I CSCux	erability in ng of list h BR Series rged Broad s could al nenticated er to cause to reload, nial of ser ion. Cisco rged Broad s running able versi OS XE are nformatio 40637. Kn	n the leaders in dband low an , remote e the resulting vice (DoS cBR-8 dband cons of affected. on: .own	co.c /cer /Cis dvis sa-2 cbr	os://tools. om/secur nter/conte coSecurit ory/cisco 0170201	ity 28 ent yA -	-CIS-IOS X- 80217/410
P: dolor			15.5(3 Fixed 1 15.6(1 15.6(2	ed Release )S 15.6(1) Releases: 1 )S1 15.6(2 )SP 16.4(2 <b>RENCE: CV</b>	S. Known 15.5(3)S2 2)S 1).				
Fidelex									
<i>Fx-2030a Firmv</i> NA	vare;Fx-2030a·	basic Fii	rmware						
Directory Traversal	13-02-2017	5	Fidelix contro to 11.5 readin allows access directo	te was dis FX-20 ser llers, vers 0.19. Arbi g via path an attack arbitrary pries on th <b>RENCE: CV</b>	ries ions prior itrary file traversal er to files and te server.	r		2	-FID-FX- 0- 80217/411
Freebsd									
<b>Freebsd</b> FreeBSD is an o stability.	operating system	n for a	variety	of platfor	ms which	n focus	es on feat	tures,	speed, and
Gain	07-02-2017	2.1	bsnmp	d, as used	lin	http	s://pierre	eki 0	-FRE-
CV 0-1 Scoring Scale	1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Denial of Service; Gain Privileges	15-02-2017	7.2	10.1, a users t service	rnel in Fre nd 10.2 al to cause a e (crash) o ially gain j	lows loca denial of or	1		FF	FRE- EEB- 80217/416
Gain Privileges	15-02-2017	7.2	in the l layer in and 10 to gain unspec <b>REFER</b> 1883	setugid sys Linux com n FreeBSD 2 allows 1 privilege cified vect RENCE: CV	patibility 9.3, 10.1 local user via ors. <b>TE-2016-</b>	., *S		FF 28	FRE- REEB- 80217/415
Overflow; Gain Privileges	15-02-2017	7.2	Integer bhyve FreeBS and 11 with a guest r local u privile device <b>REFER</b> 1889	r overflow hyperviso 5D 10.1, 10 .0 when c large amo nemory, a sers to gai ge via a cr descripto <b>RENCE: CV</b>	r in D.2, 10.3, onfigured ount of llows in afted r. <b>T-2016-</b>			FF 28	FRE- REEB- 80217/414
Bypass	15-02-2017	5	allows obtain USM au readin <b>REFER</b> <b>5677</b> The tel FreeBS 10.3, a remote argum bypass vectors "seque allocat	local user the secret uthenticat g the file. <b>RENCE: CV</b> Inetd serv SD 9.3, 10. nd 11.0 al e attackers ents to log s authentic s involving ence of me ion failure <b>RENCE: CV</b>	rs to t key for ion by <b>TE-2015-</b> ice in 1, 10.2, lows s to inject gin and cation via g a mory es."	free bsni NA		FF	FRE- REEB- 80217/413
Information			10.2, u permis	SD 9.3, 10. ses world ssions on t l.config file	-readable he	e g/20 Refe	thub.io/bl 016-01-15 erence: CV 5-5677-	- 28	REEB- 80217/412

Gain Privileges	15-02-2017	7.2	via a crafted Linux compatibility layer setgroups system call. <b>REFERENCE: CVE-2016-</b> <b>1881</b> The Linux compatibility layer in the kernel in FreeBSD 9.3, 10.1, and 10.2 allows local users to read portions of kernel memory and potentially gain privilege via unspecified vectors, related to "handling of Linux futex robust lists." <b>REFERENCE: CVE-2016-</b> <b>1880</b>	NA	0-FRE- FREEB- 280217/417
Coogla			1880		
			eveloped by Google, based o s such as smartphones and ta		and designed
NA	08-02-2017	2.9	An elevation of privilege vulnerability in Bluetooth could enable a proximate attacker to manage access to documents on the device. This issue is rated as Moderate because it first requires exploitation of a separate vulnerability in the Bluetooth stack. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32612586. <b>REFERENCE: CVE-2017- 0423</b>	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	0-GOO- ANDRO- 280217/418
Gain Information	08-02-2017	4.3	An information disclosure vulnerability in the Filesystem could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to	2017.html	0-GOO- ANDRO- 280217/419
CV 0-1 Scoring Scale	1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

			access sensitive data without permission. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-32799236. <b>REFERENCE: CVE-2017-</b> 0426		
Gain Information	08-02-2017	4.3	An information disclosure vulnerability in Audioserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access sensitive data without permission. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A- 32720785. <b>REFERENCE: CVE-2017-</b> 0425	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	0-GOO- ANDRO- 280217/420
Bypass; Gain Information	08-02-2017	4.3	An information disclosure vulnerability in AOSP Messaging could enable a remote attacker using a special crafted file to access data outside of its permission levels. This issue is rated as Moderate because it is a general bypass for a user level defense in depth or exploit mitigation technology in a privileged process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A- 32322450. <b>REFERENCE: CVE-2017- 0424</b>	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	0-GO0- ANDRO- 280217/421
Bypass; Gain Information	08-02-2017	4.3	An information disclosure vulnerability in the	https://source. android.com/se	O-GOO- ANDRO-
CV					

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

					200247/402
			Framework APIs could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32555637. <b>REFERENCE: CVE-2017-</b> 0421	curity/bulletin/ 01-02- 2017.html	280217/422
Bypass; Gain Information	08-02-2017	4.3	An information disclosure vulnerability in AOSP Mail could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A- 32615212. <b>REFERENCE: CVE-2017- 0420</b>	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	O-GOO- ANDRO- 280217/423
Bypass; Gain Information	08-02-2017	4.3	An information disclosure vulnerability in AOSP Messaging could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	O-GOO- ANDRO- 280217/424
CV					

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

			because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32807795. <b>REFERENCE: CVE-2017-</b> 0414		
Bypass; Gain Information	08-02-2017	4.3	An information disclosure vulnerability in AOSP Messaging could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32161610. <b>REFERENCE: CVE-2017- 0413</b>	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	0-GOO- ANDRO- 280217/425
Execute Code	08-02-2017	6.8	A remote code execution vulnerability in libstagefright could enable an attacker using a specially crafted file to execute arbitrary code in the context of an unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses this library. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-31999646. <b>REFERENCE: CVE-2017- 0409</b>	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	O-GOO- ANDRO- 280217/426

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

Execute Code	08-02-2017	6.8	vulner could e using a file to e code in unpriv issue is to the remote an app this lib Androi <b>REFER</b> 0408			oid.com/s y/bulletin 2- 7.html	se /	280217/4		
Denial of Service	08-02-2017	7.8	vulner DNS co remote special packet hang o is rate possib denial Androi 5.0.2, 5 7.1.1. <i>A</i> 32322	ability in l ould enabl e attacker lly crafted to cause a r reboot. 7 d as High o ility of rer of service id. Versior 5.1.1, 6.0, 6 Android IE	Bionic e a to use a network a device This issue due to the note . Product: ns: 4.4.4, 5.0.1, 7.0, D: A-	andr curit 01-0	s://source oid.com/s y/bulletin 2- 7.html	se	0-G0 ANDF 2802	
Execute Code			andr curit 01-0 2017	s://source oid.com/s y/bulletin 2- 7.html	com/se AN alletin/ 28		0- {0- 17/429			

			REFEF	17432. RENCE: CV	Æ-2017-					
Execute Code; Gain Privileges	08-02-2017	9.3	vulner Audios a local applica arbitra contex proces as Higl used to elevato which access applica Andro 5.0.2, 5 7.1.1.4 32220	h because o gain loca ed capabil are not no ible to a th ation. Proo id. Versior 5.1.1, 6.0, 6 Android II	ld enable ecute vithin the ileged ue is rated it could be al access to ities, ormally nird-party duct: ns: 4.4.4, 5.0.1, 7.0, D: A-	and curi 01-0 201	os://source roid.com/ ty/bulletin )2- 7.html	se	O-GO ANDI 2802	
Execute Code; Gain Privileges	08-02-2017	9.3	An elev vulner Audios a local applica arbitra contex proces as High used to elevato which access applica Andro 5.0.2, 9 7.1.1.4 32703	h because o gain loca ed capabil are not no ible to a th ation. Proo id. Versior 5.1.1, 6.0, 6 Android II	ld enable ecute vithin the ileged ue is rated it could be al access to ities, ormally nird-party duct: ns: 4.4.4, 5.0.1, 7.0, D: A-	and curi 01-0 201	os://source roid.com/ ty/bulletin )2- 7.html	se	O-GO ANDI 2802	
Execute Code; 08-02-2017 9.3 An eleva				levation of privilegehttps://source.0-G00-erability inandroid.com/seANDR0-						
CV 0.1										9 10

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

CV 0-	1	1-2	2-3	3-4	4-5	5-6	6-7		7-8		8-9	9-10
Execute Code; Gain Privileges	0	8-02-2017	7 9.3	vulner Medias a local applica arbitra	An elevation of privilege vulnerability in Mediaserver could enable a local malicious application to execute arbitrary code within the context of a privileged		an cui 01	https://source. android.com/se curity/bulletin/ 01-02- 2017.html		'se	0-G0 AND 2802	
Execute Code; Gain Privileges	0	8-02-2017	7 9.3	access applica Androi 5.0.2, 5 7.1.1. A 32705 <b>REFER</b> 0417 An elev vulner Audios a local applica arbitra contex proces as High used to elevato which access applica 5.0.2, 5 7.1.1. A 32886	ible to a thation. Proc id. Versior 5.1.1, 6.0, 6 Android IE 438. <b>RENCE: CV</b> vation of p ability in server cou malicious ation to ex ary code w t of a prive s. This iss n because o gain loca ed capabili are not no ible to a thation. Proc id. Versior 5.1.1, 6.0, 6 Android IE	ird-party luct: is: 4.4.4, 5.0.1, 7.0, b: A- <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b> <b>TE-2017-</b>	htt an. cui 01 20 d e o	droid	/sourc l.com/ oulleti ml	'se	0-G0 AND 2802	
	Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rat as High because it could used to gain local access elevated capabilities, which are not normally accessible to a third-par application. Product: Android. Versions: 4.4.4					ecute ithin the ileged ue is rate it could b l access t ities,	01 20 d e	rity/l -02- 17.ht	oulleti ml	n/	2802	17/432

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

CV 0-1		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9	9-10
Execute Code; Gain Privileges	08	8-02-2017	7 9.3	vulner Frame enable applica arbitra contex proces as High used to elevate which access	vation of p ability in t work APIs a local ma ation to ex ary code w t of a prive s. This iss n because o gain loca ed capabil are not no ible to a th ation. Proc	he could alicious ecute ithin the ileged ue is rated it could b l access to ities, ormally ird-party	andr curit 01-0 2012	s://sourc oid.com/ cy/bulleti 2- 7.html	se A	D-GOO ANDRC 280217	)-
Execute Code; Gain Privileges		8-02-2017		An elev vulner Frame enable applica arbitra contex proces as High used to elevate which access applica Androi 7.1.1. A 33039 <b>REFER</b> 0412	RENCE: CV	he could alicious ecute ithin the ileged ue is rated it could b l access to ities, ormally hird-party luct: hs: 7.0, h: A- <b>E-2017-</b>	andr curit 01-0 2017	7.html	se <i>A</i> n/ 2	D-GOO ANDRO 280217	)- 7/435
				as High used to elevate which access applica Androi 6.0.1, 7 ID: A-3	b ecause o gain loca ed capabil are not no ible to a th ation. Proc id. Versior 7.0, 7.1.1. A 2706020. <b>ENCE: CV</b>	l access to ities, ormally urd-party luct: us: 6.0, Android	e D				

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

			7.1.1. <i>1</i> 33042	id. Version Android IE 690. <b>RENCE: CV</b>	D: A-					
Execute Code; Gain Privileges	08-02-2017	9.3	An ele vulner Frame enable applica arbitra contex proces as Hig used to elevato which access applica Andro 5.1.1, 6	h because o gain loca ed capabil are not no	the s could alicious tecute vithin the ileged ue is rated it could be al access to ities, ormally nird-party duct: ns: 5.0.2, 7.0, 7.1.1. 1929765.	andr curit 01-0 2017	s://source oid.com/s y/bulletin 2- 7.html	se	0-G0 ANDI 2802	
Execute Code; Overflow; Memory Corruption	08-02-2017	9.3	A reme vulner Media: an atta specia cause during proces rated a possib execut contex proces libhev Andro 6.0.1, 7 ID: A-3	, media file sing. This as Critical ility of rer ion withir	Ild enable g a file to orruption e and data issue is due to the note code the ediaserver ects the Product: ns: 6.0, Android	andr curit 01-0 2017	s://source oid.com/s y/bulletin 2- 7.html	se	0-G0 ANDI 2802	
Execute Code; Overflow;	08-02-2017	9.3		ote code e ability in	xecution	-	s://source oid.com/s		O-GO ANDI	
CV										

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

Memory Corruption			an atta special cause f during proces rated a possib execut contex proces libheve Androi 6.0.1, 7 ID: A-3 <b>REFER</b> 0406	server cou acker using lly crafted memory co media file sing. This as Critical ility of ren ion within to f the Mo s. This affe c library. F id. Versior 7.0, 7.1.1. A 2915871. RENCE: CV	g a file to orruption e and data issue is due to the note code the ediaserve ects the Product: ns: 6.0, Android <b>TE-2017-</b>	01-0 2017	7.html			17/439
Execute Code; Overflow; Memory Corruption	08-02-2017	9.3	vulner Surface enable special cause f during proces rated a possib execut contex Surface Produce Versio Andro	bte code exability in eflinger co e an attack lly crafted memory co g media file ssing. This as Critical ility of rem ion within t of the eflinger pr ct: Android ns: 7.0, 7.1 id ID: A-31 <b>RENCE: CV</b>	andr curit 01-0 2012	s://sourc roid.com/ ty/bulleti 12- 7.html	se	O-GC AND 2802	-	
Execute Code	08-02-2017	10	A rema vulner Qualco could e attacke arbitra contex issue is due to	ote code ex ability in t omm crypt enable a re er to execu ary code w t of the ke s rated as the possib e code exe	the co driver emote ute rithin the rnel. This Critical pility of	andr curit 01-0 2012	s://sourc roid.com/ ty/bulleti 12- 7.html	se	0-GC AND 2802	
CV 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8-9	9-10

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	<b>9-1</b> 0
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	--------------

			Produ Versio A-326 QC-CR	ntext of th ct: Android ns: N/A. A 52894. Re #1077457 <b>RENCE: CV</b>	d. ndroid II ferences: 7.	):				
Google ; Linux										
Android / Linux Android is a mob primarily for tou monolithic Unix-l	oile operating s achscreen mob	ile devi	es such	as smart						
Gain Information	08-02-2017	2.6	An info vulner Qualco could o malicio access permis issue i becaus compr proces Versio Kernel A-317 QC-CR	ormation of ability in to omm sound enable a lo ous applica data outsi ssion level s rated as se it first ra- tomising a s. Product ns: Kernel l-3.18. And 96345. Re- #1073129 <b>RENCE: CV</b>	the d driver ocal ation to ide of its s. This Moderate equires privilege c: Android -3.10, lroid ID: ferences: 0.	andr curit 01-0 2017 d l.	s://sourc oid.com/ y/bulleti 2- 7.html	se	0-G00- ANDR0- 280217/	/442
Gain Information	08-02-2017	2.6	vulner Qualco Execut Comm enable applica outsid levels. as Moo first re compr proces Versio Kernel	ormation of ability in to omm Secur- cion Enviro unicator co a local ma ation to acc e of its per This issue derate beco equires omising a cs. Product ns: Kernel I-3.18. And 04078. Re	the ce onment ould alicious cess data mission e is rated ause it privilege the Android -3.10, lroid ID:	andr curit 01-0 2017	s://sourc roid.com/ ty/bulleti 12- 7.html	se	0-G00- ANDR0- 280217/	′443
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	-9	9-10

			-	#1076407 <b>ENCE: CV</b>						
Gain Information	08-02-2017	4.3	An information disclosure vulnerability in the NVIDIA video driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Product: Android. Versions: Kernel- 3.10. Android ID: A- 32721029. References: N- REFERENCE: CVE-2017- 0448. <b>REFERENCE: CVE-2017-</b> 0448 The aio_mount function in fs/aio.c in the Linux kernel				:://sourc oid.com/ y/bulleti 2- '.html	se	0-G0 AND 2802	
Gain Privileges; Bypass	07-02-2017	7.2	0448 The aio_mount function in			nux/ f6b4e 63a9	om/torvalds/li nux/commit/22 f6b4d34fcf039c 63a94e7670e0 da24f8575a5a			0- RO- 17/445
Denial of Service; Gain Privileges	07-02-2017	7.2				om/t nux/ 0967 e5a2	://githul corvalds/ commit/ 4e68646 4e3000b 2541220	li 97 ce 3	0-G0 AND 2802	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8-9	9-10

			multithreaded access to internal data structures for IPv4 UDP sockets. <b>REFERENCE: CVE-2014</b> <b>9914</b>	-	
Execute Code	08-02-201	7 7.6	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rate as Moderate because it first requires compromising a privileg process and is mitigated by current platform configurations. Product: Android. Versions: Kern 3.10. Android ID: A- 31707909. References: I RB#32094. <b>REFERENCE: CVE-2017</b> 0449	android.com/se curity/bulletin/ 01-02- 2017.html ed el- B-	0-G00- ANDR0- 280217/447
Execute Code	08-02-201	7 7.6	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute arbitrary code within th context of the kernel. Th issue is rated as High because it first requires compromising a privileg process. Product: Andro Versions: Kernel-3.18. Android ID: A-32919560 <b>REFERENCE: CVE-2017</b> 0447	android.com/se curity/bulletin/ 01-02- 2017.html e is ged id.	0-G00- ANDR0- 280217/448
Execute Code	08-02-201	7 7.6	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute	android.com/se	0-G00- ANDRO- 280217/449
CV 0- Scoring Scale	1 1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

CV 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8_9	9-10
Execute Code	08-02-2017	7 7.6	An elev vulner Qualco	vation of p ability in 1 mm Wi-F enable a lo	the i driver	and	os://souro roid.com, ity/bullet 02-	/se	0-GC AND 2802	
Execute Code	08-02-2017	7 7.6	vulner Realtel could e malicio execut within kernel as High require privile Produc Version	vation of p ability in t k sound di enable a lo ous applic e arbitrary the conte This issu because es compro ged proce ct: Androi ns: Kernel d ID: A-32 ENCE: CV	the river ocal ation to y code xt of the e is rated it first omising a ss. d. -3.10. 2705232.	and curi 01- 201	os://sourd roid.com, ity/bullet 02- 7.html	/se	0-GC AND 2802	
Execute Code	08-02-2017	7 7.6	Version Androi REFER 0446 An elev vulner touchs enable applica arbitra contex issue is becaus compre proces Version Androi	s. Product ns: Kernel d ID: A-32 <b>ENCE: CV</b> vation of p ability in t creen driv a local ma ation to ex try code w t of the ke s rated as the it first r omising a s. Product ns: Kernel d ID: A-32 <b>ENCE: CV</b>	-3.18. 2917445. <b>YE-2017-</b> Drivilege the HTC Ver could alicious tecute vithin the ernel. This High equires privilege t: Androio -3.18. 2769717.	http and curi 01- 201	os://souro roid.com, ty/bullet 02- 7.html	/se	0-GC AND 2802	
			contex issue is becaus compre	ry code w t of the ke s rated as e it first r omising a s. Product	ernel. This High equires privilege	d				

CV0-11-22-3ScaleImage: scaleImage: scaleImage: scaleImage: scale	3-4 4-5	5-6 6-7	7-8 8-9	9-10
--	---------	---------	---------	------

CV											
Execute Code	08	8-02-2017	7 7.6	vulner Qualco could a malicia execut within kernel as Higl requir privile Produc	vation of p ability in t omm Wi-F enable a lo ous applic e arbitrar the conte . This issu n because es compro ged proce ct: Androio ns: Kernel	the i driver ocal ation to y code xt of the e is rated it first omising a ss. d.	and curi 01-0	s://sourc roid.com/ ty/bulleti )2- 7.html	se	O-GO ANDI 2802	
Execute Code		8-02-2017		An eler vulner Qualco could e malicio execut within kernel as Higl requir privile Produc Versio Kernel A-328' QC-CR <b>REFEF</b> 0442	vation of p ability in t omm Wi-F enable a lo ous applic e arbitrary the conte . This issu n because es compro ged proce ct: Androio ns: Kernel -3.18. And 71330. Re #1092497 <b>RENCE: CV</b>	the i driver ocal ation to y code xt of the e is rated it first omising a ss. d. I-3.10, droid ID: ferences: 7. <b>YE-2017-</b>	andi curi 01-0 201	7.html	se n/		₹0- 17/453
				execut within kernel as Higl requir privile Produc Versio Kernel A-328' QC-CR	ous applic e arbitrar the conte . This issu n because es compro ged proce ct: Androi ns: Kernel -3.18. And 77494. Re #1092497	y code xt of the e is rated it first omising a ss. d. I-3.10, droid ID: ferences: 7.	201	7.html			

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

Execute Code08-02-20177.6An elevation of privileg vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android ID: A-33252788. References: Q-CGR#1095770. REFERENCE: CVE-2017- 0440https://source. android.com/se 2017.html0-GOO- ANDRO- 280217/451Execute Code08-02-20177.6An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android ID: A-33252788. References: Q-CGR#1095700 REFERENCE: CVE-2017- 0440https://source. android.com/se curity/bulletin/ 01-02-0-GOO- ANDRO- 280217/450Execute Code08-02-20177.6An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local a privileged process. Product: Android ID: A-32450647. References: Q-C-GR#1092059. RFERENCE: CVE-2017- 0439https://source. android.com/se a				A-3287 QC-CR	-3.18. And 2662. Re ‡1095009 <b>ENCE: CV</b>	ferences: 9.						
vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32450647. References: QC-CR#1092059. REFERENCE: CVE-2017- 	Execute Code	08-02-2017	7.6	vulnera Qualco could e malicio executo within kernel. as High require privile Produc Version Kernel A-3325 QC-CRa <b>REFER</b>	ability in f mm Wi-F nable a lo us applic e arbitrar the conte This issu because es compro ged proce t: Androi ns: Kernel -3.18. And 2788. Re #1095770	the i driver ocal ation to y code xt of the e is rated it first omising a ss. d. l-3.10, lroid ID: ferences: ).	ar cu 01 20	ndroio urity/ 1-02-	d.com/ bulletin	se	ANDI	R0-
vulnerability in the Qualcomm Wi-Fi driverandroid.com/se curity/bulletin/ANDRO- 280217/452	Execute Code	08-02-2017	7.6	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32450647. References: QC-CR#1092059. <b>REFERENCE: CVE-2017-</b>				ndroio urity/ 1-02-	d.com/ bulletii	se	ANDI	RO-
	Execute Code	08-02-2017	7.6	An elev vulnera Qualco	ability in t mm Wi-F	ar cu	android.com/se curity/bulletin/					

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

Execute Code08-02-20177.6An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android ID: A-32402310. References: QC-CR#1092497. REFERENCE: CVE-2017- 0437https://source. android.com/se 2017.html0-G00- ANDRO- 280217/45Execute Code08-02-20177.6An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. QC-CR#1092497. REFERENCE: CVE-2017- 04370-G00- android.com/se ANDRO- 280217/45Execute Code08-02-20177.6An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android.01-02- 2017.html04-00- 280217/45				execut within kernel as Higl require privile Produc Versio Kernel A-3240 QC-CR	bus applic e arbitrar the conte . This issu h because es compro ged proce ct: Androi ns: Kernel -3.18. And 02604. Re #1092497	y code xt of the e is rated it first omising a ss. d. I-3.10, droid ID: ferences: 7.	201	7.html			
Execute Code08-02-20177.6An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process.https://source. android.com/se (01-02- 2017.html0-GOO- ANDRO- 280217/45	Execute Code	08-02-2017	7.6	An elev vulner Qualco could e malicio execut within kernel as Higl requir privile Produc Versio Kernel A-3240 QC-CR <b>REFE</b>	ability in f omm Wi-F enable a lo ous applic e arbitrary the conte . This issu n because es compro ged proce ct: Androi ns: Kernel -3.18. And 02310. Re #1092497	the i driver ocal ation to y code xt of the e is rated it first omising a ss. d. I-3.10, Iroid ID: ferences: 7.	and curi 01-0	roid.com/s ty/bulletin )2-	e Al	NDRO-	58
Versions: Kernel-3.10,	Execute Code	08-02-2017	7.6	An elective vulner Qualco could e malicio execut within kernel as Higl require privile Produc	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android.			roid.com/s ty/bulletin )2-	e Al	NDRO-	59

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	<b>9-1</b> 0
------------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	--------------

			malicious application to execute arbitrary code	2017.html	
Execute Code	08-02-2017	7.6	An elevation of privilege vulnerability in the Synaptics touchscreen driver could enable a loca	https://source. android.com/se curity/bulletin/ 01-02-	0-G00- ANDRO- 280217/462
Execute Code	08-02-2017	7.6	Kernel-3.18. Android ID: A-31906657. References: QC-CR#1078000. <b>REFERENCE: CVE-2017-</b> 0435 An elevation of privilege vulnerability in the Synaptics touchscreen driver could enable a loca malicious application to execute arbitrary code within the context of the touchscreen chipset. This issue is rated as High because it first requires compromising a privilege process. Product: Android Versions: Kernel-3.18. Android ID: A-33001936. <b>REFERENCE: CVE-2017-</b> 0434	2017.html d	0-G00- ANDR0- 280217/461
Execute Code	08-02-2017	7.6	Kernel-3.18. Android ID: A-32624661. References: QC-CR#1078000. <b>REFERENCE: CVE-2017-</b> 0436 An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10,	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	0-G00- ANDRO- 280217/460

			within the context of the touchscreen chipset. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-31913571. <b>REFERENCE: CVE-2017-</b> <b>0433</b>		
Execute Code	08-02-2017	7.6	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31906415. References: QC-CR#1078000. <b>REFERENCE: CVE-2016-</b> 8481	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	O-GOO- ANDRO- 280217/463
Execute Code	08-02-2017	7.6	An elevation of privilege vulnerability in the Qualcomm Secure Execution Environment Communicator driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31804432. References:	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	O-GOO- ANDRO- 280217/464

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

			as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32879283. References:		
Execute Code	08-02-2017	7.6	A-32879283. References: QC-CR#1091940. <b>REFERENCE: CVE-2016-</b> <b>8476</b> An elevation of privilege	https://source.	0-G00-
			vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32451104. References: QC-CR#1087797. <b>REFERENCE: CVE-2016- 8421</b>	android.com/se curity/bulletin/ 01-02- 2017.html	ANDRO- 280217/466
Execute Code	08-02-2017	7.6	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	0-G00- ANDR0- 280217/467
CV 0-1 Scoring Scale	l 1-2	2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

			kernel. ' as High requires privileg Product Version Kernel-3 A-3245 QC-CR#	because s compro ed proce : Android s: Kernel 3.18. And 1171. Re 1087807	e is rated it first omising a ss. d. -3.10, lroid ID: ferences:				
Execute Code	08-02-2017	7.6	An eleva vulnera Qualcon could er maliciou execute within t kernel.' as High requires privileg Product Version Kernel- A-32454 QC-CR#	because s compro ed proce :: Android s: Kernel 3.18. And 4494. Re 1087209	the i driver ocal ation to y code xt of the e is rated it first omising a ss. d. -3.10, lroid ID: ferences:	and cur 01- 201	os://source roid.com/ ity/bulletin 02- .7.html	se A	-GOO- NDRO- 80217/468
Execute Code	08-02-2017	9.3	An eleva vulnera Broadco could en maliciou execute within t kernel.' as Critic possibil perman compro require operatin	cal due to ity of a lo ent devio mise, wh reflashir	the driver ocal ation to y code xt of the e is rated the ocal ce ich may ng the n to repai	and cur 01- 201	os://sourc roid.com/ ity/bulletin 02- .7.html	se A	-GOO- NDRO- 80217/469

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

			Android. Versions: Kernel- 3.10, Kernel-3.18. Android ID: A-32838767. References: B- RB#107459. <b>REFERENCE: CVE-2017- 0430</b>		
Execute Code	08-02-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel- 3.10. Android ID: A- 32636619. References: N- REFERENCE: CVE-2017- 0429. <b>REFERENCE: CVE-2017-</b> 0429	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	0-GOO- ANDRO- 280217/470
Execute Code	08-02-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel- 3.10. Android ID: A- 32401526. References: N-	https://source. android.com/se curity/bulletin/ 01-02- 2017.html	O-GOO- ANDRO- 280217/471

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

CV Scoring Scale	1-2	2-3	3-4     4-5     5-6     6-7     7-8     8-9     9-10
NA	13-02-2017	5	An issue was discovered in Honeywell XL Web II controller XL1000C500NAO-HON-XL WE- 280217/474XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 andVAVA
			Honeywell XL Web IIWE-controller XL1000C500280217/473XLWebExe-2-01-00 and280217/473prior, and XLWeb 500XLWebExe-1-02-08 andprior. Password is storedin clear text.REFERENCE: CVE-2017-5140
offering a combi	Honeywell's E nation of BACn commitment	et IP, BA to reduc	based, freely- programmable Building Automation controller Cnet MS/TP, and LONWORKS communication. It demonstrates cing total installed cost and total building lifecycle cost for rs. An issue was discovered in NA O-HON-XL
			REFERENCE: CVE-2017- 0427
Execute Code	08-02-2017	9.3	An elevation of privilege vulnerability in the kernel file system could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel- 3.10, Kernel-3.18. Android ID: A-31495866.https://source. android.com/se android.com/se android.com/se curity/bulletin/ 01-02- 2017.html0-GOO- ANDRO- 280217/472
			REFERENCE: CVE-2017- 0428. REFERENCE: CVE-2017- 0428

			disclos access becaus Storag	Any user is te a passw ing a spect te of Plaint e of a Pass RENCE: CV	ord by ific URL, text sword.				
NA	13-02-2017	6.5	An issu Honey contro XLWeb prior, a XLWeb prior, A privile and ch param specifi Improj Manag	te was dis well XL W ller XL100 DExe-2-01 and XLWe DExe-1-02 A user wit ges is able ange the eters by a c URL bec Der Privile ement. <b>RENCE: CV</b>	eb II 00C500 -00 and b 500 -08 and h low e to open ccessing a ause of ege	a		WE-	ON-XL 217/475
NA	13-02-2017	6.5	Honey contro XLWeb prior, a XLWeb prior, a establi session invalid session gives t steal a session FIXATI	te was dis well XL W ller XL10( DExe-2-01 and XLWe DExe-1-02 An attacke sh a new to n, without ating any n identifie he opport uthenticat ns (SESSIC ON). <b>RENCE: CV</b>	eb II 00C500 -00 and b 500 -08 and er can user existing r, which unity to red			WE-	ON-XL 217/476
Directory Traversal	13-02-2017	7.5	An issu Honey contro XLWeb prior, a	ie was dis well XL W ller XL100 Exe-2-01 and XLWe DExe-1-02	eb II )0C500 -00 and b 500	n NA		WE-	ON-XL 217/477
CV Scoring Scale	-1 1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	3-9	9-10
Gain Privilege	s 1	5-02-2017	7.2	could a gain rc a speci comma bellma	X 6.1, 7.1, allow a loc oot privile ally crafte and withir il client. II : IV91006	cal user to ges using ed 1 the BM	are.i x/efi y/be sory	://aix.sof bm.com/ ixes/secu ellmail_ad .asc	ai Irit	O-IBN AIX;V 2802	
<i>AIX; Vios</i> AIX is an ope Server facilita server.	-	0,0							•		,
Gain Privilege	s 0	02-02-2017	7.2	could a exploit the bel root pr	X 6.1, 7.1, allow a loc a vulnera llmail bina rivileges. RENCE: CV	al user to bility in ary to gain	are.i x/efi y/be sory	://aix.sof bm.com/ ixes/secu ellmail_ad 2.asc	ai Irit		4-AIX- 17/480
NA	0	01-02-2017	7.2	unspec that w auther obtain privile	X contain cified vuln ould allow ticated us root level ges. <b>RENCE: CV</b>	erability 7 a locally ser to	are.i x/efi y/lsi	://aix.sof bm.com/ ixes/secu ncode_ad 2.asc	ai Irit		M-AIX- 17/479
IBM AIX AIX is an oper NA		<mark>ating syster</mark> .5-02-2017	n from IB 4.9	IBM Al a local with a argum crash t APARs IV914	based on X 7.1 and user to op specially o ent that w he system : IV91488 56, IV9023 ENCE: CV	7.2 allow oen a file crafted rould h. IBM 5, IV91482 34.	rs http: are.i x/efi y/sy ory.a	://aix.sof bm.com/ ixes/secu sproc_ad	ai Irit		4-AIX- 17/478
				auther directo by acco URL. <b>REFER</b>	A user wit aticating ca ory travers essing a sp RENCE: CV	an make a sal attack pecific					

			IV9102	08, IV9101 11. RENCE: CV	·						
NA	15-02-2017	7.2	7.2 cor unspect that we auther obtain privile IV8865 IV8842 IV8805	IX 5.3, 6.1, ntains an cified vuln ould allow nticated us root level ges. IBM A 58, IV8798 19, IV8764 53. <b>RENCE: CV</b>	erability y a locally ser to APARs: 31, 40,	ar x/ y/ sc	re.ib /efix	/aix.sof m.com/ es/secu erylv_ad sc	ai rit	0-IB AIX;V 2802	
Security Access											
Security Access M IBM Security Acc											
technologies and										, un	
NA	01-02-2017	3.5	Manag proces backup update sufficie origin code, v auther load m	ecurity Acc ger for Wel ases patche os and oth es without ently verif and integr which coul nticated at alicious co <b>RENCE: CV</b>	b es, image er ying the rity of the d allow a tacker to ode.	m /c id 8	n.con docv l=sw	/www.i 1/suppc iew.wss g21995	ort ?u 51		JR- 17/483
NA	01-02-2017	4	Manag allow a user to highly inform incorre	ecurity Acc ger for Wel an authent gain acce sensitive sensitive dation due ect file per <b>RENCE: CV</b>	b could cicated ess to to rmissions	m /c id 0 s.	n.con docv	/www.i n/suppc iew.wss g21995	ort ?u	0-IB SECU 2802	
Gain Information	01-02-2017	4	IBM Se Manag allow a	ecurity Acc er for Wel an authent er to obtai	b could cicated	m /0	n.con docv	/www.i n/suppc iew.wss g21995	ort ?u	O-IB SECU 2802	
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8		8-9	9-10

Gain Information01-02-20175IBM Security Access Manager for Web could allow an unauthenticated user to gain access to sensitive information by entering invalid file names.http://www.ib mcom/support /docview.wss?u 280217/ id=swg21995340-IBM- SECUR- 280217/ id=swg2199534Gain Information01-02-20175IBM Security Access manager for Web could allow aremote attacker to obtain sensitive information due to security misconfigurations. RFFERENCE: CVE-2016- 3023http://www.ib Access m.com/support /docview.wss?u id=swg21995510-IBM- SECUR- 280217/ id=swg2199551Gain Information01-02-20172.1IBM Security Access Manager for Web allows web pages to be stored locally which can be read by another user on the system. RFFERENCE: CVE-2016- 3024http://www.ib SECUR- 280217/ id=swg21995340-IBM- SECUR- 280217/ id=swg2199534Denial of Service01-02-20175.5IBM Security Access Manager for Web allows wuch pages to be stored locally which can be read by another user on the system. RFFERENCE: CVE-2016- 3024http://www.ib mcom/support /docview.wss?u id=swg21995340-IBM- SECUR- 280217/ id=swg2199534Denial of Service01-02-20175.5IBM Security Access Manager for Web allows wulnerable to a denial of (XKE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources.0-IBM- mcom/support	CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	3-9	9-10
Cain Information01-02-20175IBM Security Access Manager for Web could allow an unauthenticated user to gain access to sensitive information by entering invalid file 		01-02-2017	5.5	Manage vulnera service Externa (XXE) e process remote exploit to expo informa all avai	er for We able to a c , caused b al Entity I error whe sing XML e attacker this vulne ose highly ation or c lable mer	b is lenial of njection n data. A could erability sensitive onsume	m.co /do id=s 0	om/suppo cview.ws	ort s?u	SECU	R-
Gain Information01-02-20175IBM Security Access Manager for Web could allow an unauthenticated user to gain access to sensitive information by entering invalid file names.http://www.ib Manager for Web could id=swg2199534 80-IBM- SECUR- 280217/ id=swg2199534 8Gain Information01-02-20175IBM Security Access Manager for Web could allow an unauthenticated user to gain access to sensitive information by entering invalid file names.http://www.ib 80-IBM- SECUR- 280217/ id=swg2199534 8Gain Information01-02-20175IBM Security Access Manager for Web could allow a remote attacker to obtain sensitive information due to security misconfigurations.http://www.ib 90-IBM- SECUR- 280217/ id=swg2199551		01-02-2017	2.1	Manage web pa locally by anot system <b>REFER</b>	er for Wel ges to be which can ther user	b allows stored 1 be read on the	m.co /do id=s	om/suppe cview.ws	ort s?u	SECU	R-
Gain Information01-02-20175IBM Security Access Manager for Web could allow an unauthenticated user to gain access to sensitive information by entering invalid file names.http://www.ib Manager for Web could id=swg2199534O-IBM- SECUR- 280217/ id=swg2199534	Information			Manage allow a obtain inform securit miscon <b>REFER</b> 3017	er for Wel remote a sensitive ation due y figuration ENCE: CV	b could ttacker to to 1s. <b>'E-2016-</b>	m.co /do id=s 9	om/suppo cview.ws swg21995	ort s?u 551	SECU 2802	R- 17/487
sensitive information from 6 error message using a specially crafted HTTP		01-02-2017	5	error n special reques <b>REFER</b> <b>3021</b> IBM Se Manage allow a user to sensitiv enterin names. <b>REFER</b>	nessage u ly crafted t. ENCE: CV curity Acc er for Wel n unautho gain acce ve inform ig invalid	sing a HTTP <b>E-2016</b> - cess b could enticated ess to ation by file	http m.co /do id=s	om/suppe cview.ws	ort s?u	SECU	R-

				RENCE: CV	Æ-2016-					
Denial of Service; Gain Information	01-02-2017	7 6.4	Bluem remote sensiti caused entity proces the XM attacke vulner arbitra system service	ngle Sign ( ix could al e attacker ve inform l by a XML (XXE) erro sing XML IL parser. er could es ability to p ary files or o r cause e. <b>RENCE: CV</b>	low a to obtain ation, external or when data by A remote xploit this read a the a denial o	m.co /doc id=s 1	://www.i om/suppo :view.wss wg21995	rt ?u	O-IBN SECU 2802	
Cross Site Request Forgery	01-02-2017	7 6.8	IBM Se Manag vulner reques could a execut unauth transn that th	ecurity Acc ger for Wel able to cro at forgery allow an a e maliciou norized ac nitted from e website <b>RENCE: CV</b>	b is oss-site which ttacker to us and tions n a user trusts.	m.co /doc id=s 5	://www.i om/suppo oview.wss wg21995	rt ?u	O-IBN SECU 2802	
Linux										
Linux Kernel	ic a monalith	vic Univ lil	to compli	toropora	ting quete	m korne	.1			
The Linux kernel Gain Information	06-02-2017		Off-by- pipe_a lib/iov kernel local u sensiti uniniti memo opport circum from a incorr decisio	one error dvance fur jiter.c in t before 4.9 sers to ob ve inform alized hea ry location cunistic stances by pipe after ect buffer-	in the nction in the Linux 9.5 allows tain ation from p- ns in y reading an release	http: om/ nux/ dc6f d1c0 n adc7	el. s://githul torvalds/ 'commit/ 65bc5e23 05fe34b50 'e8bbf1fb	li b9 32 da	O-LIN LINU 2802	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	3-9	9-10

			5550							
Gain Information	06-02-2017	2.1	functio drivers b105.c before uniniti memor log ent read th allows obtain inform log.	5_get_line n in s/usb/seri in the Lin 4.9.5 plac alized hea ry content ry upon a le line stat local user sensitive ation by r	ial/kl5ku es p- s into a failure to tus, which s to eading th	.ree ow s 14 l	ps://bugzi dhat.com/s _bug.cgi?ic 16114	sh	O-LIN LINU 2802	
Gain Information	14-02-2017	2.1	The tim Linux I 4.9.9, v CONFIG enable to disco (as disco values names) the /pr related function kernel, and the timen rt_info kernel,	G_TIMER_ d, allows l over real l tinguished inside a P pace) by r roc/timer_ l to the print n in /time/tim	ough STATS is ocal user PID value I from PII ID eading list file, int_timer er_list.c ner_set_st n ler.c.	l.on /ke /tij s /?i s 6de D a64 b09	p://git.ker rg/cgit/ling ernel/git/t p.git/comn d=dfb4357 dbdf57d58 4361c9d79 e0b1	ix ip nit 'da 3b	O-LIN LINU 2802	
Gain Privileges	3.6	functio in the I 4.9.6 p bit dur involvi filesyst local us	nple_set_a n in fs/po Linux kerr reserves t ing a setxa ng a tmpfa sem, which sers to gai ges by lev	osix_acl.c nel before he setgid attr call s h allows in group	om nu 7d 0d	ps://githu a/torvalds/ x/commit/ e07d89c14 76a15bec2 f24a2a89f3	li 49 1 bb	O-LIN LINU 2802		
CV Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8		8-9	<b>9-1</b> 0

CV											
Denial of Service	C	06-02-2017	4.9	The nested functio	_vmx_chee on in 86/kvm/v	-	.red ow_	os://bugz hat.com, bug.cgi?i 7812	/sh	O-LII LINU 2802	
Denial of Service; Overflow	0	06-02-2017	4.9	in drivers _gem.c DRM d kernel not set upon c detecti local u denial pointe OOPS) size va VC4_SI	4_get_bcl f s/gpu/drm in the Vid river in th before 4.9 an errno ertain ove ons, which sers to cau of service r derefere via incons lues in a JBMIT_CL ENCE: CV	n/vc4/vc eoCore e Linux 9.7 does value erflow h allows use a (incorrec nce and sistent ioctl call.	.red 4 ow <u></u> 141	os://bugz hat.com/ bug.cgi?i 6437	/sh	O-LII LINU 2802	
Denial of Service; Gain Privileges		96-02-2017	4.6	progra on exe NOTE: exists i incomp 2016-7 <b>REFER</b> <b>5551</b> The load_so implent arch/x in the i 4.9.5 in a "MOV instruct guest ( denial crash) privile applica <b>REFER</b>	egment_denentation 86/kvm/e Linux kerr nproperly / SS, NULL ction, whic OS users to of service or gain gu ges via a c	strictions issions. rability f an r CVE- <b>TE-2017-</b> <b>Escriptor</b> in emulate.c remulate.c remulates selector ch allows o cause a (guest OS rafted	http .red ow_ 141	os://bugz hat.com/ bug.cgi?i 4735	/sh	O-LII LINU 2802	

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

CV									0.0	
Service				Linux keri		-	'torvalds/		LINU	
Denial of Service; Overflow; Memory Corruption	6-02-2017	4.9	fs/cifs the Lin before incorr CONFI option users t service memo possib other i use of virtual scatter <b>REFER</b> 10154	RENCE: CV	ypt.c in 4.9.x racts the STACK lows local denial of crash or cion) or specified leveragin n one a <b>YE-2016-</b>	om/ nux, deed cc94 76e	s://githul /torvalds/ /commit/ ec77a5a68 lb21a8a9 lb21a8a9 42176685	li 06 39 1a 5d	O-LIN LINU 2802	X- 17/500
Denial of Service	6-02-2017	4.9	function fs/ext4 Linux 1 does n meta b allows proxim cause a (out-o system ext4 in <b>REFER</b> 10208	4/super.c kernel thr ot proper plock grou physically nate attacl a denial of f-bounds n crash) vi nage. RENCE: CV B	in the ough 4.9.8 ly validate ps, which wers to Service read and a a craftee <b>/E-2016-</b>	.red ow_ 3 139	s://bugzi hat.com/s bug.cgi?id 5190	sh =		X- 17/499
			4.9.8 in the VM which guest ( denial memo levera mishan referen	mproperly IXON instr allows KV OS users to of service ry consum ging the ndling of p	ruction, M L1 o cause a (host OS option) by page					

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

CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	3-9	9-10			
Denial of Service; Memory Corruption	06-02-2017	7.2	atusb.o 4.9.x b incorro CONFI	drivers/net/ieee802154/ atusb.c in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local			b.c in the Linux kernell.cbefore 4.9.6 interacts/kcrectly with thevaFIG_VMAP_STACKco			//git.kern /cgit/linu nel/git/to s/linux.gi mit/?id=0 lefa4bdf6	ıx or t/ )5	O-LIN LINU 2802	
Service; Overflow			drivers _gem.c DRM d kernel local u denial possib other i size va VC4_SI <b>REFEF</b> 5576	vc4_get_bcl function in drivers/gpu/drm/vc4/vc4.redha ow_bu jem.c in the VideoCoreDRM driver in the Linux kernel before 4.9.7 allows local users to cause a denial of service or possibly have unspecified other impact via a crafted size value in a VC4_SUBMIT_CL ioctl callredha ow_bu 14164REFERENCE: CVE-2017			=		17/503				
Denial of Service Denial of	14-02-2017   5     0   14-02-2017   5     0   0   7     0   0   7     0   0   7		process, which allows local users to cause a denial of service (system crash) by leveraging access to this process group.REFERENCE: CVE-2010- 53285The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options. REFERENCE: CVE-2017- 59707.2Integer overflow in the				https://patchw ork.ozlabs.org/ patch/724136/			J- X- 17/502			
			signals	does not p s with a pr ID of zero	ocess	2755	/commit/ 5e20ab0c 99c2dc7c2	72	2802	17/501			

			users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.2a150e3f27dc6 fcf0a9ad5655REFERENCE: CVE-2017- 55482a150e3f27dc6 fcf0a9ad5655	
Denial of Service; Memory Corruption	06-02-2017	7.2	drivers/hid/hid-corsair.chttps://github.cO-Iin the Linux kernel 4.9.xom/torvalds/liLIN	LIN- NUX- 0217/505
Denial of Service	06-02-2017	7.2	randomization feature in om/torvalds/li LIN	LIN- NUX- 0217/506
Denial of Service;	06-02-2017	7.2	The crypto scatterlist API https://github.c 0-1	LIN- NUX-
CV				

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

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

managed Layer 2	switch functio	ns.								
NA	13-02-2017	5	Moxa I Secure	ie was dis EDR-810 I Router. B	ndustrial <sup>By</sup>		A		E	D-MOX- DR-8- 80217/510
				ing a spec m resourc						
			· ·	on the we		a				
				ous user is configura						
				s (PRIVIL						
				ATION).	JE 2016					
			8346	RENCE: CV	E-2010-					
Miineport E1 Fir	mware; Miine	port E2 F		e; Miinep	ort E3 Fi	rmwa	are			
Moxa's MiiNePor										ant to add
sophisticated net								ration ef		MOY
NA	13-02-2017	5		ie was dis MiiNePort		in N	A		-	)-MOX- /IINE-
				ns prior to						80217/511
				ns prior to						/-
				sions prio						
			U	uration da						
				in a file th	nat is not					
			encryp	RENCE: CV	/F.2016.					
			9346		E-2010-					
NA	13-02-2017	5	Moxa I	ie was dis MiiNePort	E1	in N	ΙA		Ν	)-MOX- /IINE-
				ns prior to					2	80217/512
				ns prior to sions prio						
				acker may		0				
				orce an ac						
				1 cookie to						
				nload con	ifiguratio	n				
			files.	RENCE: CV	/E-2016-					
			9344		2 2010					
Netapp						•				
Data Ontap										
Clustered Data O	•	-	-	ge control	lers, or r	nodes	s, ma	naged a	is a si	ngle logical
pool so your oper Gain	ations scale m	ore easily		p Data ON	TAD	h	ttpa	//kb.ne	ta C	D-NET-
Information	07-02-2017	4.5	· ·	9 Data ON 8.2.4P5, v			-	n/supp		O-NET-
				ing in 7-M			•	ticle/N		80217/513
CV 0.1	1.0	2.2	2.4		E C		7	7.0	0.4	
Scoring 0-1 Scale	1-2	2-3	3-4	4-5	5-6	6-'		7-8	8-9	9 9-10

Execute Code	07-02-2017	6.5	obtain information about the volumes configured for HTTP access.0REFERENCE: CVE-2016- 6495064950NetApp OnCommand System Manager 8.3.x0before 8.3.2 allows remote authenticated users to execute arbitrary code via unspecified vectors.0		te t/	ttps:, p.cor /inde nten	0001 https://kb.neta pp.com/suppor t/index?page=c ontent&id=901 0070		0-NE DAT <i>I</i> 2802		
			REFER	RENCE: CV							
Samsung			8322								
Samsung Mobile											
Samsung helps yo		vide rang	e of hon	ne electro	nics with	cutti	ing-e	dge tec	hno	logy in	cluding
smartphones, tab	lets, TVs, home	applian	ces and i	more.							
Denial of Service Denial of	13-02-2017	2.1	Samsung devices with Android KK(4.4) or L(5.0/5.1) allow local users to cause a denial of				http://security. samsungmobile. com/smrupdate .html#SMR- JAN-2016 http://security.			0-SA SAMS 2802	SU- 17/515
Service	13-02-2017	5	Androi L(5.0/ attacke of serv via a cr TvoutS	Samsung devices with Android KK(4.4), L(5.0/5.1), or M(6.0) allow attackers to cause a denial of service (system crash) via a crafted system call to TvoutService_C. <b>REFERENCE: CVE-2016-</b>		sa w co al .h Fl o	amsu om/s	ingmob mrupd SMR-	ile.	SAMS	
Schneider Electr	ric										
Homelynk Contro NA	oller Lss10010	0 Firmw	vare								
Execute Code; Cross Site Scripting	13-02-2017	4.3	An issue was discovered in Schneider Electric homeLYnk Controller, LSS100100, all versions prior to V1.5.0. The homeLYnk controller is			in N	NA			0-SCH- HOMEL- 280217/517	
CV 0-1 Scoring Scale	1-2	2-3	3-4	4-5	5-6	6-2	7	7-8	8	8-9	9-10

			susceptible to a cross-site scripting attack. User inputs can be manipulated to cause execution of JavaScript code. <b>REFERENCE: CVE-2017-</b> <b>5157</b>		
Sendquick		<b>F</b> ( <b>C</b>			
	v allows a comp	uter to se	<b>ms Gateway Firmware</b> end or receive Short Message	e Service (SMS) tra	nsmissions to
NA	05-02-2017	5	An issue was discovered on SendQuick Entera and Avera devices before 2HF16. An attacker could request and download the SMS logs from an unauthenticated perspective. <b>REFERENCE: CVE-2017-</b> <b>5137</b>	NA	O-SEN- AVERA- 280217/518
Execute Code	05-02-2017	7.5	An issue was discovered on SendQuick Entera and Avera devices before 2HF16. Multiple Command Injection vulnerabilities allow attackers to execute arbitrary system commands. <b>REFERENCE: CVE-2016-</b> <b>10098</b>	NA	O-SEN- AVERA- 280217/519
NA	05-02-2017	7.8	An issue was discovered on SendQuick Entera and Avera devices before 2HF16. The application failed to check the access control of the request which could result in an attacker being able to shutdown the system. <b>REFERENCE: CVE-2017-</b> <b>5136</b>	NA	O-SEN- AVERA- 280217/520

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