Ndurc	National C	- 101041		CI	/E Rep	ort			Vol. 04		
Vulnerability Type(s)	Publish Date	CVSS			& CVE			Patch	1	N II	CIIPC
			Ap	plicat	ion (A	.)					
Acer											
Acer Portal											
NA	08-06-2017	4.3	3.9.4. prope certif attac the-n SSL c	2000 for early value icates, kers to hiddle a ertifica	app befor Andridate SS which a performattack value.	oid doe SL llows r n a Mar ia a cra	emote ı-in-	NA		A	-ACE- CER - 10617/ 1
Adblock			_					•			
Adblock											
NA	08-06-2017	6.4	remo arbit webs block	te attac rary res ites and ring filte	ore 2.22 ckers to sources d to disa ers.	block on arb able art	itrary	com/ chadl mmit ea776	://github kzar/wat olock/co :/5b77de e0eff2aa7 722d64fl b985	t A 2: 6 0: 7	-ADB- DBLO- 10617/ 2
AMD								1			
Fglrx-driver											
Gain Privileges	07-06-2017	7.2	allow Privil attac exists for C CVE	rs local legesile k. NOTI s due to VE-201 I D: CVE		o gain G a symli vulnera omplete 7724	ain nk bility e fix	NA		F	-AMD- GLRX- 10617/ 3
Gain Privileges	07-06-2017	7.2	allow Privil attac	AMD fglrx-driver before 15.7 allows local users to gain Gain Privilegesileges via a symlink attack. CVE ID: CVE-2015-7723				NA		F	-AMD- GLRX- 10617/ 4
Ansibleworks											
Ansible											
Execute Code	08-06-2017	6.5	The user module in ansible https://githu		://github	o. A	-ANS-				
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1

CV Scoring Scale	(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
NA	12-06-2017	5	Apac	he NiFi	before	0.7.4 a	nd 1.x	NA		A	-APA-
XSS	12-06-2017	4.3	In Apache NiFi before 0.7.4 and 1.x before 1.3.0, there are certain user input components in the UI which had been guarding for some forms of XSS issues but were insufficient. CVE ID: CVE-2017-7665				NA		N	-APA- IFI- 10617/ 9	
Nifi	100000	1.6	- -					1		1 -	
Hadoop NA	04-06-2017	8.5	alpha Linux docke insuf When enable	ache Hand in the dominar in ache Hand in ach	3.0.0-almerExemands and value of the control of the	pha2, t cutor reas root alidatio ature is ted use oot.	he ins with n.	NA		Н	-APA- (AD00- 10617/ 8
Hadoon			servi				01	f- fediz. mit;h	git;a=co =f65c96 e3c1851 e7e49fc3	m 1 d	,
DoS	07-06-2017	5	CXF I befor	cation j Fediz be e 1.2.1 kers to	efore 1. allow r	1.3 and emote	1.2.x	wip- us.ap	://git- ache.org	C 2	-APA- XF F- 10617/
Apache Cxf Fediz											
NA	07-06-2017	7.2	conno befor escap via a	throot, jection pection pection pection pection in the content pection in the content pection	olugins allow l tricted k attack	in ansi ocal uso environ c.	ers to	a.redl	://bugzi nat.com, bug.cgi?i 3468	/s A	-ANS- NSIB- 10617/ 6
			authe arbit	e 1.6.6 enticate rary con	ed users mmand	S.		nsible /8ed6 8229	ansible/ e/comm 6350e65 2a631f0 faacffe7f	it 2 c 0 8	NSIB- 10617/ 5

			before 1.3.0 need to establish the response header telling browsers to only allow framing with the same origin. CVE ID: CVE-2017-7667
Ranger			
NA	14-06-2017	4.3	In environments that use external location for hive tables, Hive Authorizer in Apache Ranger before 0.7.1 should be checking RWX permission for create table. CVE ID: CVE-2017-7677 https://cwiki.a pache.org/conf luence/display /RANGE-210617/ 11 https://cwiki.a pache.org/conf luence/display /RANGER/Vul nerabilities+fo und+in+Range r
NA	14-06-2017	4.3	Apache Ranger before 0.6.3 policy engine incorrectly matches paths in certain conditions when policy does not contain wildcards and has recursion flag set to true. CVE ID: CVE-2016-8746 https://cwiki.a pache.org/conf luence/display /RANGER/Vul nerabilities+fo und+in+Range r
NA	14-06-2017	7.5	Policy resource matcher in Apache Ranger before 0.7.1 ignores characters after '*' wildcard character - like my*test, test*.txt. This can result in unintended behavior. CVE ID: CVE-2017-7676 https://cwiki.a pache.org/conf luence/display /RANGER/Vul nerabilities+fo und+in+Range r
Tomcat	06.06.0045	_	m
NA	06-06-2017	5	The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default
CV Scoring Scale	e (CVSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Ty			

CV Scoring Scale (CVS	<u> </u>	0-1	1-2	use a de	3-4	4-5	5-6	6-7	7-8		9	9-10
DoS	07-06-2017	5	through 1.3, the secure self- hosted invasive debug interface allows normal world attackers to cause a denial of service com/ARM- software/arm- trusted- firmware/wiki									
Arm Trusted Fi								1				
ARM												
Ws-xmlrpc DoS	06-06-2017	4.3	defaute by a Second HTTF used that to dispar regar CVE ITTHE CONTROLL AND ADDRESS A LATER TO THE CONTROLL A LATER TO THE CONTR	Ilt, the reserved of the second of the secon	responsidoes de de Custr pages a GET re f the acteriore in walte attacervice (a) by de containing	se general percent of the percent of	on the viets ensure ethod. TP oc chiva cause ce essing	NA			A-AI WS-2 2106 15	
			8.5.14 7.0.0 Depereque unexy resul inclus config repla custo other (1) U other HTTF pages they as a 0	4, 8.0.0. to 7.0.7 ending of est this pected a triangle of the second of	RC1 to 77 did n the o could le and und the Defi to permit or removed by the could be splicitly SPs ignored. JSPs must en any erruest, re	ot do the riginal ead to desirable or page aultSer loval of Notes for coded ore the used as a sure the or dispersive the egardles	and his. le es vlet is s, the or pages: the s error at atch					

			CVE ID: CVE-2017-9519 us/arti	cles/11 20
Atmail CSRF	08-06-2017	6.8	allowing an attacker to create a mail.co user account. mail.co	/help.at A-ATM- m/hc/e ATMAI- 210617/
Asterisk Certified Asteri NA Atmail	sk;0pen Source 02-06-2017	5		/bugs.d A-AST- org/863 CERTI- 210617/ 19
Clearpass Sql	08-06-2017	7.5	ClearPass Policy Manager 6.5.x ubanet	16-
Bypass Arubanetwork	07-06-2017 s	6.8	In ARM Trusted Firmware 1.3, RO memory is always executable at AArch64 Secure EL1, allowing attackers to bypass the MT_EXECUTE_NEVER protection mechanism. This issue occurs because of inconsistency in the number of execute-never bits 2	y- ry-TFV- /github. A-ARM- RM- ARM T- re/arm- 210617/ 17 ire/wiki Trusted- are-

								Minor 7-8-0	169147- -Update -2- eSync-2-	e-	
CSRF	08-06-2017	6.8	allow the Sl all en	ring an MTP ho nails.	attacke	2 has Car to cha er to cha e and hi -9518	nge	https: mail.c n- us/ar 50072 Minor 7-8-0	//help.acom/hc/ ticles/1 169147- Update -2- eSync-2-	/e 1 - e-	A-ATM- ATMAI- 210617/ 21
CSRF	08-06-2017	6.8	allow and in	ing an mport i			-	mail.c n- us/ar 50072 Minor 7-8-0	//help.acom/hc/ ticles/1 169147- Update -2- eSync-2-	/e 1 - e-	A-ATM- ATMAI- 210617/ 22
Bigtreecms											
Bigtree Cms	1	1									
Directory Traversal	04-06-2017	5	vulne core\ ensio BigTr Wind read a seque parar	erability admin' ns\file- ree CMS ows, al arbitra ences in ences in neter.	brows throughowing files the di	in levelope er.php i gh 4.2.1 attacke via\ rectory	n 8 on ers to	com/l ms/B CMS/ 9	//githu bigtreec igTree- issues/2	28	A-BIG- BIGTR- 210617/ 23
Execute Code; Sql	04-06-2017	6.5	BigTr allow users comm core\ \mod creat	ree CMS s remo to executation to exe	S throug te auth cute arl via \modul esigner	rability gh 4.2.1 enticate bitrary les\dev \form- acker cr e at	8 ed SQL eloper	com/ ms/B	//githu bigtreec igTree- issues/2	;	A-BIG- BIGTR- 210617/ 24
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	9 9-10
CV Scoring Scale (CVSS) Vulnerability Type(s):											

			gner, at ad statis nal=t	n/deve/and the min/da stics/in- rue. ID: CVE	ie injec shboar tegrity,	tion is v d/vital 'check/	<i>r</i> isible s-				
Sql	05-06-2017	6.5	throu authors SQL is crafted mani packated and core \packated NOTI must packated as the write	SPUTEI igh 4.2. enticate njection ed table fest.jso age. Thi admin admin cadmin insions tages\i E: the ve implicit age or e ey all ha e PHP fil	18 allowed users object in an in an is issue \modul \modul \modul \modul \modul \rendor settly trustextension ave the les."	ws rem s to con s via a t in upload exists i es\dev proces tates "Y st any on you i ability	ed in eloper ss.php eloper php.	com/l ms/B	//githu bigtree igTree- issues/	С	A-BIG- BIGTR- 210617/ 25
Execute Code	05-06-2017	6.5	throu author arbit crafts PHP extra filena cache This core and core NOTI must packs as the	SPUTEI igh 4.2. enticate rary coo ed pack web sho ction of me pat e/packa issue ex admin cadmin kages\i enticage or e ey all ha e PHP fi	18 allowed users de by u age corell, rela f a ZIP acterns suge/xxxxxists in \modul \install \install \rendor suge/xxxxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxists in \modul \install \rendor suge/xxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxxists in \modul \install \rendor suge/xxxists in \modul \install \rendor \text{install \rendor suge/xxxists} \tag{x}	ws rem s to exe ploadin ntaining ted to archive uch as yyy.pl es\dev unpac unpack tates "Y st any on you i	ote cute ig a g a to hp. eloper eloper php. You	com/l ms/B	//githu bigtree igTree- issues/	С	A-BIG- BIGTR- 210617/ 26
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	9 9-10

			CVE I	D: CVE	-2017	9442						
Execute Code Sql	06-06-2017	6.5	BigTr allow users comm core/ /mod The a table admi: ws/c: visibl modu page/	ree CMS rs remo to execute ands v admin lules/v ttacker name a n/deve reate/ e at ad les/vie / or adr	/modul iews/cr create	gh 4.2.1 enticat citrary es/dev eate.pl s a craf module injection ax/auto archabl odules_	8 ed SQL eloper np. red s/vie on is o- e-	com/ ms/B	://githu bigtree igTree- issues/	c		BIG- TTR- 0617/
CSRF	02-06-2017	6.8	BigTr the cl core\ d\vita and ti core\ d\vita 301.p	ee CMS ear pai admin als-stat he fron admin als-stat	RF issues through the content of the	gh 4.2.1 to es\das 404\cle parame es\das 404\cre	8 - hboar ar.php ter to hboar	com/ ms/B	://githu bigtree igTree- issues/	с		BIG- GTR- D617/
CSRF	02-06-2017	6.8	CSRF throw parar /adm for ex /adm ce=fa unloc	exists and the exists and exist and	in BigT 18 with o es/revi es/revi	ree CM: the for sions.p sions/ ch id=1	rce hp - 1/?for	com/ ms/B CMS/ 17d0 0c21	://githubigtreeigTree-commi9b05d94ee2f4f	t/c bc2 bb	BIG	BIG- TTR- D617/
CSRF	05-06-2017	6.8	CSRF core\ file\u user i index ckage packa	BigTree CMS through 4.2.18 has CSRF related to the com/big core\admin\modules\users\pro file\update.php script (modify user information), the index.php/admin/developer/pa ckages/delete/ URI (remove packages), the index.php/admin/developer/up							BIG	BIG- FTR- D617/
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	8-9	9-10

			grade/ignore/?versions= URI, and the index.php/admin/developer/up grade/set-ftp-directory/ URI. CVE ID: CVE-2017-9444		
Execute Code Bypass	02-06-2017	7.5	Unrestricted File Upload exists in BigTree CMS through 4.2.18: if an attacker uploads an 'xxx.pht' or 'xxx.phtml' file, they could bypass a safety check and execute any code. CVE ID: CVE-2017-9364	https://github. com/bigtreec ms/BigTree- CMS/commit/ b7229394695 1cc650eaf51f5 d2f62ceac6335 e12	A-BIG- BIGTR- 210617/ 31
Bluecoat					
Advanced Secui	re Gateway;Ca	cheflow;	Proxysg		
Bypass	08-06-2017	5	Blue Coat Advanced Secure Gateway 6.6, CacheFlow 3.4, ProxySG 6.5 and 6.6 allows remote attackers to bypass blocked requests, user authentication, and payload scanning. CVE ID: CVE-2016-6594	https://bto.blu ecoat.com/sec urity- advisory/sa13 0	A-BLU- ADVAN- 210617/ 32
Bluez					
Bluez					
		4.6	Buffer overflow in BlueZ 5.41	https://git.ker	A-BLU-
Execute Code; Overflow	09-06-2017		and earlier allows an attacker to execute arbitrary code via the parse_line function used in some userland utilities. CVE ID: CVE-2016-7837	nel.org/pub/sc m/bluetooth/b luez.git/commi t/?id=8514068 150759c1d6a4 6d4605d2351 babfde1601	BLUEZ- 210617/ 33
Overflow Call-cc	09-06-2017		execute arbitrary code via the parse_line function used in some userland utilities.	m/bluetooth/b luez.git/commi t/?id=8514068 150759c1d6a4 6d4605d2351	210617/
Overflow	09-06-2017		execute arbitrary code via the parse_line function used in some userland utilities.	m/bluetooth/b luez.git/commi t/?id=8514068 150759c1d6a4 6d4605d2351	210617/
Overflow Call-cc	09-06-2017	5	execute arbitrary code via the parse_line function used in some userland utilities.	m/bluetooth/b luez.git/commi t/?id=8514068 150759c1d6a4 6d4605d2351	210617/

CV Scoring Scale (CVSS	S)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Execute Code	08-06-2017	7.2	A vulnerability in how DLL files are loaded with Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to install and run an executable file with Gain Privilegesileges equivalent to the Microsoft Windows SYSTEM account. The vulnerability is due to incomplete input validation of path and file names of a DLL file before it is loaded. An attacker could exploit this vulnerability by creating a malicious DLL file and installing it in a specific system directory. A successful exploit could allow the attacker to execute commands on the underlying Microsoft Windows host with Gain Privilegesileges equivalent to the SYSTEM account. The attacker would need valid user credentials to exploit this vulnerability. This vulnerability affects all Cisco AnyConnect Secure Mobility Client for Windows software versions prior to 4.4.02034. Cisco Bug IDs: CSCvc97928. CVE ID: CVE-2017-6638	https://tools.ci sco.com/securi ty/center/cont ent/CiscoSecur ityAdvisory/cis co-sa- 20170607- anyconnect	A-CIS- ANYCO- 210617/ 36
Cisco <i>Anyconnect Sec</i>	cure Mohility Cl	lient			
XSS	06-06-2017	4.3	irc.cgi in CGI:IRC before 0.5.12 reflects user-supplied input from the R parameter without proper output encoding, aka XSS. CVE ID: CVE-2017-8920	http://cgiirc.or g/	A-CGI- CGI- 210617/ 35
CGI					
Cgiirc			CVE ID: CVE-2017-9334		
			application that calls "length" on it.		

Elastic Services	Controller				
NA	13-06-2017	6.5	A vulnerability in the ConfD CLI of Cisco Elastic Services Controllers could allow an authenticated, remote attacker to log in to an affected system as the admin user, aka an Insecure Default Administrator Credentials Vulnerability. More Information: CSCvc76661. Known Affected Releases: 2.2(9.76). CVE ID: CVE-2017-6689	https://tools.ci sco.com/securi ty/center/cont ent/CiscoSecur ityAdvisory/cis co-sa- 20170607- esc5	A-CIS- ELAST- 210617/ 37
NA	13-06-2017	9	A vulnerability in Cisco Elastic Services Controllers could allow an authenticated, remote attacker to log in to an affected system as the Linux root user, aka an Insecure Default Password Vulnerability. More Information: CSCvc76631. Known Affected Releases: 2.2(9.76). CVE ID: CVE-2017-6688	https://tools.ci sco.com/securi ty/center/cont ent/CiscoSecur ityAdvisory/cis co-sa- 20170607- esc4	A-CIS- ELAST- 210617/ 38
Email Security A	Appliance				
Bypass	13-06-2017	5	A vulnerability in the email message scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured filters on the device, as demonstrated by the Attachment Filter. More Information: CSCvd34632. Known Affected Releases: 10.0.1-087 9.7.1-066. Known Fixed Releases: 10.0.2-020 9.8.1-015. CVE ID: CVE-2017-6671	https://tools.ci sco.com/securi ty/center/cont ent/CiscoSecur ityAdvisory/cis co-sa- 20170607- esa1	A-CIS- EMAIL- 210617/ 39
Firesight System		5	A vulnerability in the feature-	https://tools.ci	A-CIS-
Firesight System Bypass	13-06-2017	0-1	license management functionality of Cisco Firepower	sco.com/securi ty/center/cont	FIRES- 210617/ 3-9 9-10

			System Software could allow an unauthenticated, remote attacker to bypass URL filters that have been configured for an affected device. More Information: CSCvb16413. Known Affected Releases: 6.0.1 6.1.0 6.2.0 6.2.1. Known Fixed Releases: 6.2.1 6.2.0.1 6.1.0.2. CVE ID: CVE-2017-6674	ent/CiscoSecur ityAdvisory/cis co-sa- 20170524-fmc	40				
Industrial Netw	ork Director								
XSS	13-06-2017	4.3	Vulnerability in the web interface of Cisco Industrial Network Director could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against an affected system. More Information: CSCvd25405. Known Affected Releases: 1.1(0.176). CVE ID: CVE-2017-6675	https://tools.ci sco.com/securi ty/center/cont ent/CiscoSecur ityAdvisory/cis co-sa- 20170607-ind	A-CIS- INDUS- 210617/ 41				
Prime Data Cen	T								
Gain Privileges	08-06-2017	10	Vulnerability in Cisco Prime Data Center Network Manager (DCNM) Software could allow an unauthenticated, remote attacker to log in to the administrative console of a DCNM server by using an account that has a default, static password. The account could be granted root- or system-level Gain Privileges. The vulnerability exists because the affected software has a default user account that has a default user account that has a default user account is created automatically when the software is installed. An attacker could exploit this vulnerability by connecting remotely to an affected system and logging in to the affected	https://tools.ci sco.com/securi ty/center/cont ent/CiscoSecur ityAdvisory/cis co-sa- 20170607- dcnm2	A-CIS- PRIME- 210617/ 42				
CV Scoring Scale (CVSS		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8 8	9-10				
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable									

			software by using the credentials for this de account. A successful could allow the attact this default user account in to the affected soft gain access to the adconsole of a DCNM software related to Release 10.2(1) for Windows, Linux, and Appliance platforms. IDs: CSCvd95346.	efault user l exploit ker to use ount to log tware and ministrative erver. This Cisco Prime to Manager leases prior r Microsoft l Virtual Cisco Bug			
Execute Code	08-06-2017	10	Vulnerability in the raccess control (RBAC functionality of Cisco Center Network Man (DCNM) could allow unauthenticated, renattacker to access seinformation or executode with root Gain Privilegesileges on as system. The vulneral to the lack of authentiauthorization mechadebugging tool that winadvertently enable affected software. Ar could exploit this vulby remotely connect debugging tool via To successful exploit couthe attacker to access information about the software or execute a code with root Gain Privilegesileges on the system. This vulneration Cisco Prime Data Cer Network Manager (Executed Control of C	ole-based c) Prime Data lager an note nsitive Ite arbitrary In affected oility is due tication and nisms for a was Id in the In attacker Inerability Ing to the Ing t	sco.co ty/cer ent/C	0607-	A-CIS- PRIME- 210617/ 43
CV Scoring Scale (CVSS) Vulnerability Type(s):)	0-1	1-2 2-3 3-4	4-5 5-6	6-7	7-8	9-10

Telepresence Ce DoS	2 Software; Tel 08-06-2017	epresen 7.8	Linux, a platform CSCvd0 CVE ID: Ce Tc Soy Vulnera Initiation Cisco Te and Coll Softwar unauther attacker endpoir resultin (DoS) control the soft exploit is sending packets. An explatacker availabit of the discomplet vulnera following platform softwar 7.3.8 an CSCux9.	te CVE-2017 ftware ability in the on Protocol elePresence laboration le could allocation. The couse and to reload ag in a denial ondition. The bility is due not much a ware. An atthis vulneray a flood of State to the affect oit could allocation to impact ility of service, included to the could allocate to the affect oit could allocate to impact ility of service, included to the could allocate to impact ility of service, included to the could allocate to the affect oit could allocate to impact ility of service, included to the could allocate to impact ility of service, included to the could allocate to the could allocate to impact ility of service, included to the could allocate to the could al	oft Wind Appliance IDs: 2-6639 2-663	n Sthe (TC) esence ctedly, vice ck of within could y TE rice.	sco.co ty/cer ent/C ityAdv co-sa-	//tools.c m/secur nter/con iscoSecu visory/ci	ri T t 2 r 4	A-CIS- PELEP- 10617/
Ultra Services F	ramework Ele	ment M		CVL 2017	0010					
NA	13-06-2017	6.5	A vulnerability in Cisco Ultra Services Framework Element Manager could allow an authenticated, remote attacker with access to the management network to log in to the affected device using default credentials present on the system, aka an				sco.co ty/cer ent/C		ri U t 2 r 4	I-CIS- JLTRA- 10617/ 5
CV Scoring Scale (CVSS) Vulnerability Type(s): DoS- Denial of Service;		0-1 nest Forgery	; XSS- Cross	2-3 3-4 Site Scripting; S	4-5 Sql- SQL Inj	5-6 ection; NA:	6-7 Not Appli	7-8 cable	8-9	9-10

5)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-1 (
08-06-2017	5	Cloud Foundry Diego 0.1468.0 through 0.1470.0 allows remote attackers to cause a denial of service.	http://www.o penwall.com/li sts/oss- security/2016	A-CLO- DIEGO- 210617/ 49
,		CVL 1D. CVL 2017-0100		
		Gain Privileges via a symlink attack on a temporary file.	g/2.5.0	48
08-06-2017	4.6	Unspecified tests in Lynis before 2.5.0 allow local users to write to arbitrary files or possibly gain	https://github. com/CISOfy/ly nis/releases/ta	A-CIS- LYNIS- 210617/
		G. L. ID. G. L. ZUIT 0072	<u> </u>	
		Releases: 21.0.v0.65839.		
		CSCvd85710. Known Affected		
		Account Information	usf6	
		Gain Privilegesileges of the root	co-sa- 20170607-	
		to log in to the device with the	ityAdvisory/cis	47
		Manager could allow an	ty/center/cont	210617/
13-06-2017	9	A vulnerability in Cisco Ultra Services Framework Element	https://tools.ci	A-CIS- ULTRA-
		Known Affected Releases: 21.0.0. CVE ID: CVE-2017-6686		
		Information: CSCvc76699.		
		aka an Insecure Default	usf4	
		=	co-sa- 20170607-	
		with access to the management	ityAdvisory/cis	40
		Manager could allow an	ty/center/cont	210617/ 46
13-06-2017	6.5	A vulnerability in Cisco Ultra Services Framework Element	https://tools.ci	A-CIS- ULTRA-
		Releases: 21.0.0. CVE ID: CVE-2017-6687		
		CSCvc76695. Known Affected		
	08-06-2017	08-06-2017	Releases: 21.0.0. CVE ID: CVE-2017-6687 13-06-2017 6.5 A vulnerability in Cisco Ultra Services Framework Element Manager could allow an authenticated, remote attacker with access to the management network to log in as an admin or oper user of the affected device, aka an Insecure Default Credentials Vulnerability. More Information: CSCvc76699. Known Affected Releases: 21.0.0. CVE ID: CVE-2017-6686 13-06-2017 9 A vulnerability in Cisco Ultra Services Framework Element Manager could allow an authenticated, remote attacker to log in to the device with the Gain Privilegesileges of the root user, aka an Insecure Default Account Information Vulnerability. More Information: CSCvd85710. Known Affected Releases: 21.0.v0.65839. CVE ID: CVE-2017-6692 08-06-2017 4.6 Unspecified tests in Lynis before 2.5.0 allow local users to write to arbitrary files or possibly gain Gain Privileges via a symlink attack on a temporary file. CVE ID: CVE-2017-8108 08-06-2017 5 Cloud Foundry Diego 0.1468.0 through 0.1470.0 allows remote attackers to cause a denial of service.	Releases: 21.0.0. CVE ID: CVE-2017-6687 A vulnerability in Cisco Ultra Services Framework Element Manager could allow an authenticated, remote attacker with access to the management network to log in as an admin or oper user of the affected device, aka an Insecure Default Credentials Vulnerability. More Information: CSCvc76699. Known Affected Releases: 21.0.0. CVE ID: CVE-2017-6686 13-06-2017 9 A vulnerability in Cisco Ultra Services Framework Element Manager could allow an authenticated, remote attacker to log in to the device with the Gain Privilegesileges of the root user, aka an Insecure Default Account Information Vulnerability. More Information: CSCvd85710. Known Affected Releases: 21.0.v.0.65839. CVE ID: CVE-2017-6692 08-06-2017 4.6 Unspecified tests in Lynis before 2.5.0 allow local users to write to arbitrary files or possibly gain Gain Privileges via a symlink attack on a temporary file. CVE ID: CVE-2017-8108 08-06-2017 5 Cloud Foundry Diego 0.1468.0 through 0.1470.0 allows remote attackers to cause a denial of service. https://tools.ci sco.com/securi ty/center/cont ent/CiscoSecuri ty/dvisory/cis co-sa- 20170607- usf6 https://tools.ci sco.com/securi ty/center/cont ent/CiscoSecuri ty/dvisory/cis co-sa- 20170607- usf6 https://tools.ci

			CVE ID: CVE-2016-3091	/05/17/8	
Codecabin					
Wp Live Chat S	upport				
XSS	09-06-2017	4.3	Cross-site scripting vulnerability in WP Live Chat Support prior to version 7.0.07 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. CVE ID: CVE-2017-2187	https://plugins .trac.wordpres s.org/changese t/1658232/	A-COD- WP LI- 210617/ 50
Cryptopp					
Crypto++					
NA	05-06-2017	5	Crypto++ (aka cryptopp) through 5.6.5 contains an out-of- bounds read vulnerability in zinflate.cpp in the Inflator filter. CVE ID: CVE-2017-9434	http://openwa ll.com/lists/os s- security/2017 /06/06/2	A-CRY- CRYPT- 210617/ 51
Cybozu					
Dezie					
Bypass Gain Information	09-06-2017	5	Cybozu Dezie 8.0.0 to 8.1.1 allows remote attackers to bypass access restrictions to obtain an arbitrary DBM (Cybozu Dezie proprietary format) file via unspecified vectors. CVE ID: CVE-2016-7832	https://suppor t.cybozu.com/j a- jp/article/974 2	A-CYB- DEZIE- 210617/ 52
Bypass	09-06-2017	6.4	Cybozu Dezie 8.0.0 to 8.1.1 allows remote attackers to bypass access restrictions to delete an arbitrary DBM (Cybozu Dezie proprietary format) file via unspecified vectors. CVE ID: CVE-2016-7833	https://suppor t.cybozu.com/j a- jp/article/974 1	A-CYB- DEZIE- 210617/ 53
Garoon					
CSRF	09-06-2017	4.3	Cross-site request forgery (CSRF) vulnerability in Cybozu Garoon 3.0.0 to 4.2.2 allows remote attackers to hijack the authentication of a logged in user to force a logout via unspecified vectors. CVE ID: CVE-2016-4909	https://suppor t.cybozu.com/j a- jp/article/945 9	A-CYB- GAROO- 210617/ 54
CV Scoring Scale (CVS	S)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8 8	9-10
Vulnerability Type(s) DoS- Denial of Service		iest Forgery	7; XSS- Cross Site Scripting; Sql- SQL Injection; NA	: Not Applicable	

XSS	09-06-2017	4.3	in Cy allow arbit "Mes Garo	s-site so bozu Ga rs remo rary we sages" f on Keita (D: CVE	aroon 3 te attace b scrip function	.0.0 to ckers to t or HT n of Cyl	4.2.2 inject ML via	t.cybo a-	//supp zu.com ticle/95	ı/j	A-CYF GARO 21062 55	0-
Execute Code; Sql	09-06-2017	6.5	Cybo allow attacl SQL o "Mult	njection zu Garc s remo kers to comman tiRepor (D: CVE	oon 3.0. te auth execut nds via t" func	0 to 4.2 enticate arbitr	2.2 ed	t.cybo a-	//supp ozu.com cicle/94	ı/j	A-CYE GARO 21062 56	0-
CSRF	09-06-2017	6.8	Cybozu Garoon 3.0.0 to 4.2.2 allow remote attackers to obtain CSRF tokens via unspecified vectors. CVE ID: CVE-2016-4907				t.cybo a-	//supp ozu.com ticle/94	ı/j	A-CYE GARO 21062 57	0-	
Dest-unreach												
Socat		1	•					T				
DoS	08-06-2017	5	imple 1.7.3. remo denia or cra	ignal ha ementar 0 and 2 te attac d of ser ash). (D: CVE	tions in 2.0.0-b8 ckers to vice (p	allow cause rocess	a	a.redl	//bugz nat.com oug.cgi? 5711	/s	A-DES SOCA' 21062 58	T-
Digium												
Certified Asteris	sk; Open Sourc	e										
DoS Overflow	02-06-2017	5	PJSIP, as used in Asterisk Open Source 13.x before 13.15.1 and 14.x before 14.4.1, Certified Asterisk 13.13 before 13.13-cert4, and other products, allows remote attackers to cause a denial of service (buffer overflow and application crash) via a SIP packet with a crafted CSeq header in conjunction with a Via header that lacks a branch parameter. CVE ID: CVE-2017-9372				ource 13.x before 13.15.1 and 4.x before 14.4.1, Certified asterisk 13.13 before 13.13-ert4, and other products, allows emote attackers to cause a lenial of service (buffer verflow and application crash) ia a SIP packet with a crafted Seq header in conjunction with Via header that lacks a branch arameter.				A-DIG CERT 21062 59	I-
CV Scoring Scale (CVSS))	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	.9	9-10

DoS	02-06-2017	5	The multi-part body parser in PJSIP, as used in Asterisk Open Source 13.x before 13.15.1 and 14.x before 14.4.1, Certified Asterisk 13.13 before 13.13-cert4, and other products, allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet. CVE ID: CVE-2017-9359	http://downlo ads.asterisk.or g/pub/security /AST-2017- 003.txt	A-DIG- CERTI- 210617/ 60
Dnstracer Proj	ect				
Dnstracer					
DoS Overflow	05-06-2017	7.5	Stack-based buffer overflow in dnstracer through 1.9 allows attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a command line with a long name argument that is mishandled in a strcpy call for argv[0]. An example threat model is a web application that launches dnstracer with an untrusted name string. CVE ID: CVE-2017-9430	NA	A-DNS- DNSTR- 210617/ 61
Dolibarr					
Dolibarr					
Sql	05-06-2017	7.5	Dolibarr ERP/CRM before 5.0.3 is vulnerable to a SQL injection in user/index.php (search_supervisor and search_statut parameters). CVE ID: CVE-2017-9435	https://github. com/Dolibarr/ dolibarr/com mit/70636cc5 9ffa1ffbc0ce3d ba315d7d9b83 7aad04	A-DOL- DOLIB- 210617/ 62
Elastic				1	
X-pack					
NA	05-06-2017	6.5	Elastic X-Pack Security versions 5.0.0 to 5.4.0 contain a Gain Privilegesilege escalation bug in the run_as functionality. This bug prevents transitioning into the specified user specified in a	https://discuss .elastic.co/t/el astic-stack-5- 4-1-and-5-3-3- security- updates/8795	A-ELA-X- PAC- 210617/ 63
CV Scoring Scale (CVSS	5)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-10
Vulnerability Type(s): DoS- Denial of Service		uest Forger	y; XSS- Cross Site Scripting; Sql- SQL Injection; NA	a: Not Applicable	

CV Scoring Scale (CVSS Vulnerability Type(s):					
Execute Code Sql	13-06-2017	6.5	SQL injection vulnerability in the Event List plugin 0.7.8 for WordPress allows an	http://dtsa.eu/ CVE ID: CVE- 2017-9429-	A-EVE- EVENT- 210617/
Event List Proje	ect				
		T.J	in DERAEMON-CMS version 0.8.9 and earlier allows remote attackers to inject arbitrary web script or HTML via the parameters hostname, database and username. CVE ID: CVE-2016-7813	cms.com/new1	DERAE- 210617/ 66
Deraemon-cms XSS	09-06-2017	4.3	Cross-site scripting vulnerability	http://emon-	A-EMO-
Emon-cms					
Information			affected by a Cross Site Scripting (XSS) bug in the Time Series Visual Builder. This bug could allow an attacker to obtain sensitive information from Kibana users. CVE ID: CVE-2017-8439	lastic.co/comm unity/security	KIBAN- 210617/ 65
XSS; Gain	05-06-2017	4.3	page that could allow an attacker to obtain sensitive information from or perform destructive actions on behalf of other Kibana users. CVE ID: CVE-2017-8440 Kibana version 5.4.0 was	https://www.e	A-ELA-
XSS; Gain Information	05-06-2017	4.3	Starting in version 5.3.0, Kibana had a cross-site scripting (XSS) vulnerability in the Discover	https://www.e lastic.co/comm unity/security	A-ELA- KIBAN- 210617/
Elasticsearch <i>Kibana</i>					
			contains the _user properties, the behavior of run_as will be incorrect. Additionally if the run_as user specified does not exist, the transition will not happen. CVE ID: CVE-2017-8438		
			run_as request. If a role has been created using a template that	2	

		pages.edit_form.php in flatCore 1.4.6 allows remote attackers to inject arbitrary JavaScript via the PATH_INFO in an acp.php URL, due to use of unsanitized \$_SERVER['PHP_SELF'] to generate URLs. CVE ID: CVE-2017-9451	CMS/commit/f 1b42b338693a 9c240182e76e f2131057f2c2a 87	210617/ 70
		1.4.6 allows remote attackers to inject arbitrary JavaScript via the PATH_INFO in an acp.php URL, due to use of unsanitized	CMS/commit/f 1b42b338693a 9c240182e76e f2131057f2c2a	
		vulnerability in	com/flatCore/f latCore-	FLATC-
06-06-2017	4.3	Cross site scripting (XSS)	https://github.	A-FLA-
		CVE ID: CVE-2017-6512		
		vectors involving directory- permission loosening logic.	,	
		Perl allows attackers to set the	e-Path-	210617/ 69
01-06-2017	4.3	Race condition in the rmtree and remove_tree functions in the	http://cpansearch.perl.org/sr	A-FIL- FILE
•				
		webpage. CVE ID: CVE-2016-7831		
		for Mac 4.5.3 and earlier (Mac App Store) may allow a remote attacker to spoof the URL display via a specially crafted		210617/ 68
09-06-2017	5.8	Sleipnir 4 Black Edition for Mac 4.5.3 and earlier and Sleipnir 4	NA	A-FEN- SLEIP-
		id parameter to wp- admin/admin.php. CVE ID: CVE-2017-9429	8-blind-based- sql-injection-	
	ject lule 01-06-2017	ject lule 01-06-2017 4.3	admin/admin.php. CVE ID: CVE-2017-9429 09-06-2017 5.8 Sleipnir 4 Black Edition for Mac 4.5.3 and earlier and Sleipnir 4 for Mac 4.5.3 and earlier (Mac App Store) may allow a remote attacker to spoof the URL display via a specially crafted webpage. CVE ID: CVE-2016-7831	arbitrary SQL commands via the id parameter to wp-admin/admin.php. CVE ID: CVE-2017-9429 09-06-2017 5.8 Sleipnir 4 Black Edition for Mac 4.5.3 and earlier and Sleipnir 4 for Mac 4.5.3 and earlier (Mac App Store) may allow a remote attacker to spoof the URL display via a specially crafted webpage. CVE ID: CVE-2016-7831

			HTML via the currentHTMLURL parameter. CVE ID: CVE-2017-7384	reflected-xss- in-flippdf.html	
Freedesktop					
Poppler DoS; Overflow	02-06-2017	4.3	In Poppler 0.54.0, a memory leak vulnerability was found in the function Object::initArray in Object.cc, which allows attackers to cause a denial of service via a crafted file. CVE ID: CVE-2017-9408	https://bugs.fr eedesktop.org/ show_bug.cgi?i d=100776	A-FRE- POPPL- 210617/ 72
DoS; Overflow	02-06-2017	4.3	In Poppler 0.54.0, a memory leak vulnerability was found in the function gmalloc in gmem.cc, which allows attackers to cause a denial of service via a crafted file. CVE ID: CVE-2017-9406	https://bugs.fr eedesktop.org/ show_bug.cgi?i d=100775	A-FRE- POPPL- 210617/ 73
NA	06-06-2017	4.3	poppler through version 0.55.0 is vulnerable to an uncontrolled recursion in pdfunite resulting into potential denial-of-service. CVE ID: CVE-2017-7515	https://bugs.fr eedesktop.org/ show_bug.cgi?i d=101208	A-FRE- POPPL- 210617/ 74
Gnome					
Libcroco DoS Overflow	12-06-2017	4.3	The cr_tknzr_parse_comment function in cr-tknzr.c in libcroco 0.6.12 allows remote attackers to cause a denial of service (memory allocation error) via a crafted CSS file. CVE ID: CVE-2017-8834	NA	A-GNO- LIBCR- 210617/ 75
DoS	12-06-2017	7.1	The cr_parser_parse_selector_core function in cr-parser.c in libcroco 0.6.12 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted CSS file. CVE ID: CVE-2017-8871	NA	A-GNO- LIBCR- 210617/ 76
GNU				•	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s):										

Glibc					
Execute Code Overflow	12-06-2017	7.5	nscd in the GNU C Library (aka glibc or libc6) before version 2.20 does not correctly compute the size of an internal buffer when processing netgroup requests, possibly leading to an nscd daemon crash or code execution as the user running nscd. CVE ID: CVE-2014-9984	https://source ware.org/bugz illa/show_bug. cgi?id=16695	A-GNU- GLIBC- 210617/ 77
Libssp					
Overflow	07-06-2017	4.6	Binaries compiled against targets that use the libssp library in GCC for stack smashing protection (SSP) might allow local users to perform buffer overflow attacks by leveraging lack of the Object Size Checking feature. CVE ID: CVE-2016-4973	https://bugzill a.redhat.com/s how_bug.cgi?id =1324759	A-GNU- LIBSS- 210617/ 78
Goldplugins					
Testimonials Pl	ugin Easy Test	imonial	's		
Execute Code; Sql	12-06-2017	6.5	SQL injection vulnerability in the WP-Testimonials plugin 3.4.1 for WordPress allows an authenticated user to execute arbitrary SQL commands via the testid parameter to wp-admin/admin.php. CVE ID: CVE-2017-9418	http://dtsa.eu/ wp- testimonials- wordpress- plugin-v-3-4-1- union-based- sql-injection- sqli/	A-GOL- TESTI- 210617/ 79
Google					
Chrome					
DoS; Memory	06-06-2017	4.3	Double-free vulnerability in	https://gist.git	A-GOO- CHROM-
Corruption			libavformat/mov.c in FFMPEG in Google Chrome 41.0.2251.0 allows remote attackers to cause a denial of service (memory corruption and crash) via a crafted .m4a file. CVE ID: CVE-2015-1207	hub.com/bittor rent3389/8fee 7cdaa73d1d35 1ee9	210617/ 80
			Google Chrome 41.0.2251.0 allows remote attackers to cause a denial of service (memory corruption and crash) via a crafted .m4a file.	rent3389/8fee 7cdaa73d1d35	210617/
Corruption			Google Chrome 41.0.2251.0 allows remote attackers to cause a denial of service (memory corruption and crash) via a crafted .m4a file.	rent3389/8fee 7cdaa73d1d35	210617/
Corruption)	0-1	Google Chrome 41.0.2251.0 allows remote attackers to cause a denial of service (memory corruption and crash) via a crafted .m4a file.	rent3389/8fee 7cdaa73d1d35 1ee9	210617/

Overflow	04-06-2017	7.5	Google gRPC before 2017-04-05 has an out-of-bounds write caused by a heap-based buffer overflow related to core/lib/iomgr/error.c. CVE ID: CVE-2017-9431	NA	A-GRP- GRPC- 210617/ 81
H20 Project					
H20					
Gain Information	09-06-2017	6.4	Use-after-free vulnerability in H2O allows remote attackers to cause a denial-of-service (DoS) or obtain server certificate Gain Privilegesate keys and possibly other information. CVE ID: CVE-2016-7835	https://github. com/h2o/h2o/ issues/1144	A-H2O- H2O- 210617/ 82
IBM	·				
Bigfix Security	Compliance An	alytics			
XSS	07-06-2017	4.3	IBM Endpoint Manager for Security and Compliance 1.9.70 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. IBM X-Force ID: 123430. CVE ID: CVE-2017-1178	http://www.ib m.com/suppor t/docview.wss ?uid=swg2200 4164	A-IBM- BIGFI- 210617/ 83
NA	08-06-2017	4.3	IBM BigFix Compliance Analytics 1.9.79 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 123431. CVE ID: CVE-2017-1179	http://www.ib m.com/suppor t/docview.wss ?uid=swg2200 4161	210617/ 84
NA	07-06-2017	5	IBM BigFix Compliance (TEMA SUAv1 SCA SCM) 1.9.70 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user	http://www.ib m.com/suppor t/docview.wss ?uid=swg2200 4168	A-IBM- BIGFI- 210617/ 85
CV Scoring Scale (CVS	SS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

or acorning acate (CV3	9)										
CV Scoring Scale (CVS	9	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	
NA	07-06-2017	5		Domino an atta			uld		//www n/supp		A-IBM- DOMIN-
Domino											
Danie			and 6 allow obtai abou userr a URI	te EP26 5.0.5 before remo- in sensite tintern names v	fore 6.0 te attac tive info al casev ia vecto	.5.5 iFiz kers to ormatio worker ors rela	x5 on	1698	uid=sw 548	gZ	88
Gain Information	08-06-2017	5	Curai Mana	m Unive m Socia	l Progra t (SPM)	am 6.0 SP:	2	01.ibi	//www n.com/ /docvie	'su ew	A-IBM- CURAM- 210617/
Curam Social F	rogram Manag	gement									
			crafte the lo allow sensi Force	ker cou ed URL ocal syst the att tive info e ID: 11 (D: CVE	to spec tem, wh acker to ormatio 9618.	ify a file nich cou o obtain on. IBM	e from ild n	4036			
Gain Information	07-06-2017	5	Foun could inclu	Predicti dation (l allow a de arbit	(former a remot crary fil	rly PMQ e attacl es. A re	ker to mote	m.cor t/doc	//www n/supp view.w swg220	or	A-IBM- COGNO- 210617/ 87
Cognos Busine.								Ι,		.,	
DoS	07-06-2017	6.8	Intell vulne cause Entity when remo could to conresource services	Cognos igence erable to an proces te authorsume arces ance. IBM	10.1 and a denion (XX sing XI enticate this viall avail at X-Forc	d 10.2 if al of se external E) erro ML data ed attace able CF e a denie ED: 11	rvice, r . A ker ility U al of	m.cor t/doc	//www n/supp view.w swg220	or	A-IBM- COGNO- 210617/ 86
Cognos Busine.	ss Intelligence		CVE	D: CVE	-2017-	1196					
			1236	71.		ce ID:					

			credentials using multiple sessions and large amounts of data using Domino TLS Key Exchange validation. IBM X-Force ID: 117918. CVE ID: CVE-2016-6087	t/docview.wss ?uid=swg2200 2808	210617/ 89
Maximo Asset	Management				
Execute Code	13-06-2017	6.5	IBM Maximo Asset Management 7.5 and 7.6 could allow a remote authenticated attacker to execute arbitrary commands on the system as administrator. IBM X-Force ID: 120276. CVE ID: CVE-2016-9984	http://www.ib m.com/suppor t/docview.wss ?uid=swg2199 8608	A-IBM- MAXIM- 210617/ 90
Maximo Asset l	Management;M	laximo A	Asset Management Essentials		
NA	07-06-2017	6.5	IBM Maximo Asset Management 7.1, 7.5, and 7.6 could allow a remote attacker to hijack a user's session, caused by the failure to invalidate an existing session identifier. An attacker could exploit this vulnerability to gain access to another user's session. IBM X-Force ID: 120253. CVE ID: CVE-2016-9977	http://www.ib m.com/suppor t/docview.wss ?uid=swg2200 3981	A-IBM- MAXIM- 210617/ 91
Rational Rhaps	sody Design Ma	nager			l
DoS	08-06-2017	7.5	IBM Rhapsody DM 4.0, 5.0, and 6.0 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 #: 1999960. CVE ID: CVE-2016-9698	http://www.ib m.com/suppor t/docview.wss ?uid=swg2200 2258	A-IBM- RATIO- 210617/ 92
Security Key Li	fecycle Manage	er; Tivol	i Key Lifecycle Manager		
	08-06-2017	5	IBM Tivoli Key Lifecycle Manager does not require that	http://www.ib m.com/suppor	A-IBM- SECUR-
NA			users should have strong passwords by default, which	t/docview.wss ?uid=swg2199	210617/ 93
NA CV Scoring Scale (CVS		0-1	_	?uid=swg2199	•

Vulnerability Type(s			
CV Scoring Scale (CV	(\$\$)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Gain	08-06-2017	5	IBM WebSphere Application http://www.ib A-IBM-
Websphere Ap	oplication Serve	r	
			Force ID: 125731. CVE ID: CVE-2017-1319
			session (SSL) cookie. IBM X- 2002871
			secure attribute in encrypted .wss?uid=swg2 97
			Manager 6.2 is affected by a vulnerability due to a missing port/docview 210617/
NA	08-06-2017	5	IBM Tivoli Federated Identity http://www-
Tivoli Federat	ted Identity Man	ager	
			CVE ID: CVE-2016-9991
			website trusts. IBM X-Force ID: 121314.
			transmitted from a user that the
			unauthorized actions
			execute malicious and 1998167
			cross-site request forgery which could allow an attacker to pport/docview 210617/
			9.2 through 9.5 is vulnerable to 01.ibm.com/su STERL-
CSRF	08-06-2017	6	IBM Sterling Order Management http://www- A-IBM-
Sterling Sellin	ng And Fulfillmen	nt Found	
			history. IBM X-Force ID: 116136. CVE ID: CVE-2016-5959
			logs, referrer header or browser
			access to the URLs via server
			unauthorized parties have
			URL parameters. This may lead roinformation disclosure if 2092 95
			stores sensitive information in t/docview.wss 210617/
Information			Identity Manager 2.0.2 and 2.1.0 m.com/suppor SECUR-
Gain	07-06-2017	5	IBM Security Gain Privileges http://www.ib A-IBM-
Security Gain	Privileges Ident	ity Man	
			unintended actors. CVE ID: CVE-2016-6098
			be read or modified by
			way that allows that resource to 7958
			specifies permissions for a t/docview.wss 210617/security-critical resource in a ?uid=swg2199 94
			Manager 2.0.1, 2.5, and 2.6 m.com/suppor SECUR-
NA	08-06-2017	5.5	IBM Tivoli Key Lifecycle http://www.ib A-IBM-
			CVE ID: CVE-2016-6093
			makes it easier for attackers to compromise user accounts.

			reque attacl inform	ests cou ker to o nation.	ld allov btain s	ensitiv	ote	t/doc	n/supp view.w swg219	SS		3SP- 617/
Igcb												
Intellect Digital (1					1			ı	
XSS	07-06-2017	4.3	vulne Arena softw	rability Intelle are.	ripting v in Inte ect Core -2015-	ellect De banki	0	NA			A-IG INT 210 99	
Imagemagick												
Imagemagick												
DoS Overflow	02-06-2017	4.3	Readl mpc.o denia via a	MPCIm allows l of ser crafted	gick 7.0 age fun attack vice (m file. -2017-	ction in ers to c emory	ause a	com/l gick/I	//githu ImageM mageM ssues/	la la	A-IN IMA 210	
DoS Overflow	02-06-2017	4.3	Readl palm. a den leak)	PALMInc allow ial of seving a cr	gick 7.0 mage fu s attacl ervice (afted fi -2017-	nction kers to memor le.	in cause	com/l gick/I	//githu ImageM ImageM ssues/	la la	A-IN IMA 210 100	GE- 617/
DoS Overflow	02-06-2017	4.3	Readl icon.c cause (mem	CONIm::452 al a deni aory lea	gick 7.0 nage fur lows at al of ser lk) via a -2017-	nction i tackers rvice a crafte	n s to	com/l gick/l	//githu ImageM ImageM ssues/	la la	A-IN IMA 210 101	
DoS Overflow	05-06-2017	4.3	memo functi coder attacl service	ory lead on Reads/psd.c kers to ce via a	gick 7.0 k was for dPSDC: c, which cause a crafted -2017-	ound in hannel a allows denial l file.	in S	com/l gick/I	//githu ImageM mageM ssues/	la la	A-IN IMA 210 102	GE- 617/
DoS Overflow	05-06-2017	4.3	In Ima memo functi	ageMag ory leal on Rea	gick 7.0 k was fo dPDBIi c, whicl	.5-5, a ound in nage ir	l	com/l gick/l	//githu ImageM mageM ssues/	la la	A-IN IMA 210 103	
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	{	3-9	9-10

ar bearing beare (arb	٥,				
CV Scoring Scale (CVS		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8 8	9-10
Gain Information	09-06-2017	4.3	Hands-on Vulnerability Learning Tool "AppGoat" for Web Application V3.0.2 and earlier allow remote attackers to obtain	http://jvn.jp/e n/jp/JVN3212 0290/index.ht ml	A-IPA- APPGO- 210617/ 108
Appgoat					
IPA			CVE ID. CVE-2017-3003		
			users to execute arbitrary SQL commands via the jobid parameter to wpadmin/edit.php. CVE ID: CVE-2017-9603		107
Wp Jobs Execute Code; Sql	13-06-2017	6.5	SQL injection vulnerability in the WP Jobs plugin before 1.5 for WordPress allows authenticated	NA	A-INT- WP JO- 210617/
Intensewp					
Intongovim			file. CVE ID: CVE-2017-9499	171d342c6315 f44	
			assertion failure was found in the function SetPixelChannelAttributes, which allows attackers to cause a denial of service via a crafted	com/ImageMa gick/ImageMa gick/commit/7 fd419441bc71 03398e313558	IMAGE- 210617/ 106
DoS	07-06-2017	4.3	CVE ID: CVE-2017-9500 In ImageMagick 7.0.5-7 Q16, an	https://github.	A-IMA-
			the function ResetImageProfileIterator, which allows attackers to cause a denial of service via a crafted file.	gick/ImageMa gick/issues/50 0	210617/ 105
DoS	07-06-2017	4.3	In ImageMagick 7.0.5-8 Q16, an assertion failure was found in	https://github. com/ImageMa	A-IMA- IMAGE-
			assertion failure was found in the function LockSemaphoreInfo, which allows attackers to cause a denial of service via a crafted file. CVE ID: CVE-2017-9501	com/ImageMa gick/ImageMa gick/commit/0 1843366d6a7b 96e22ad7bb67 f3df7d9fd4d5d 74	IMAGE- 210617/ 104
DoS	07-06-2017	4.3	CVE ID: CVE-2017-9439 In ImageMagick 7.0.5-7 Q16, an	https://github.	A-IMA-
			attackers to cause a denial of service via a crafted file.	0	

NA				local files via unspecified vectors. CVE ID: CVE-2017-2180		
NA 09-06-2017 6.8 Hands-on Vulnerability Learning Tool "AppGoat" for Web Application V3.0.2 and earlier allow remote attackers to obtain local files via unspecified vectors, a different vulnerability than CVE-2017-2179 and: CVE-2017-2182. CVE ID: CVE-2017-2181 Execute Code 09-06-2017 6.8 Hands-on Vulnerability Learning Tool "AppGoat" for Web Application V3.0.2 and earlier allows remote code execution via unspecified vectors, a different vulnerability than CVE-2017-2181. Irssi Overflow 06-06-2017 5 In Irssi before 1.0.3, when receiving certain incorrectly quoted DCC files, it tries to find the terminating quote one byte before the allocated memory. Thus, remote attackers might be able to cause a crash. CVE ID: CVE-2017-9469 NA 06-06-2017 5 In Irssi before 1.0.3, when receiving a DCC message without source nick/host, it attempts to dereference a NULL. The state of the property of the processing	NA	09-06-2017	6.8	Tool "AppGoat" for Web Application V3.0.2 and earlier allow remote attackers to obtain local files via unspecified vectors, a different vulnerability than CVE-2017-2179 and CVE-2017-2181.	n/jp/JVN0140 4851/index.ht	APPGO- 210617/
Tool "AppGoat" for Web Application V3.0.2 and earlier allows remote code execution via unspecified vectors, a different vulnerability than CVE-2017-2181 and: CVE-2017-2182. CVE ID: CVE-2017-2179 In Irssi before 1.0.3, when receiving certain incorrectly quoted DCC files, it tries to find the terminating quote one byte before the allocated memory. Thus, remote attackers might be able to cause a crash. CVE ID: CVE-2017-9469 NA O6-06-2017 In Irssi before 1.0.3, when receiving certain incorrectly quoted DCC files, it tries to find the terminating quote one byte before the allocated memory. Thus, remote attackers might be able to cause a crash. CVE ID: CVE-2017-9469 NA O6-06-2017 In Irssi before 1.0.3, when receiving a DCC message without source nick/host, it attempts to dereference a NULL attempts to dereference and the number of the numb	NA	09-06-2017	6.8	Hands-on Vulnerability Learning Tool "AppGoat" for Web Application V3.0.2 and earlier allow remote attackers to obtain local files via unspecified vectors, a different vulnerability than CVE-2017-2179 and: CVE-2017-2182.	n/jp/JVN2087 0477/index.ht	APPGO- 210617/
Overflow Overfl	Execute Code	09-06-2017	6.8	Tool "AppGoat" for Web Application V3.0.2 and earlier allows remote code execution via unspecified vectors, a different vulnerability than CVE-2017-2181 and: CVE-2017-2182.	n/jp/JVN8023 8098/index.ht	APPGO- 210617/
Overflow Obellia 1.0.3 In Irssi before 1.0.3, when receiving certain incorrectly quoted DCC files, it tries to find the terminating quote one byte before the allocated memory. Thus, remote attackers might be able to cause a crash. CVE ID: CVE-2017-9469 NA Obellia 1.2 2.3 3.4 4.5 5.6 6.7 7.8 8.9 9.10						
NA 06-06-2017 5 In Irssi before 1.0.3, when receiving a DCC message g/security/irss IRSSIwithout source nick/host, it attempts to dereference a NULL xt 113		06-06-2017	5	receiving certain incorrectly quoted DCC files, it tries to find the terminating quote one byte before the allocated memory. Thus, remote attackers might be able to cause a crash.	g/security/irss i_sa_2017_06.t	IRSSI- 210617/
0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	NA	06-06-2017	5	In Irssi before 1.0.3, when receiving a DCC message without source nick/host, it	g/security/irss i_sa_2017_06.t	IRSSI- 210617/
LV Scoring Scale (LVSS)	CV Scoring Scale (CVS	S)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-10

Jamroom			serve	rs can	s, remo cause a - 2017	crash.						
Jamroom Jamroom												
XSS	04-06-2017	4.3	in Jan Statu	nroom s Upda	ripting before te field:	4.2.7 v		NA			JAN	AM- IRO- 1617/
Lenovo												
Active Protection	on System											
DoS	04-06-2017	4.9	Syste attack Privil to the contr denia syste hardy	m befo ker wit eges co syster oller, w l of ser m or th vare fu	ctive Preserve 1.82 In local ould serve embed to commerce attention attenti	.0.14, a Gain and com bedded ould ca cack on y to alt ality.	mands use a the	t.leno s/en/	://supp vo.com /produc ity/LEN 7	/u :t_	ACT	617/
Lenovo Service								_				
NA	04-06-2017	5	versions signated code explote a forg	on 4, a ture ve signing ited by ged cod	certifi	nd in ton logicate concept.	he c of the uld be o insert	t.leno s/en/	://supp vo.com produc ity/LEN	/u :t_	LEN	EN- NOV- 1617/
info	04-06-2017	5	version connection send mach produced serve	on 4, ar ection i system ine typ ict nan rs.	ervice In insect so used serial end reference to Le	re HT' by LSB numbe nodel a	ΓΡ to r, ind	t.leno s/en/ secur 1014		/u :t_ √-	210 117	NOV- 1617/ '
CSRF	04-06-2017	6.8	vulne Bridg explo acces	rability e befor ited by s to the	reques in Ler e versi an atta DHCP m when	ovo Se on 4 co ocker w server	ervice ould be with oused	t.leno s/en/	://supp vo.com productity/LEN	/u :t_	LEN	EN- NOV- 0617/
CV Scoring Scale (CVSS	5)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

CV Scoring Scale (CVS	S)	0-1	1-2 2-3 3-4 4-5 5-6 6-7	7 7-8	9-10
DoS Overflow	12-06-2017	4.3	quicktime_user_atoms_read_ato xplo m function in useratoms.c in db.o	os://www.e oit- com/exploit 2148/	A-LIB- LIBQU- 210617/ 123
DoS; Overflow	12-06-2017	4.3	function in lqt_quicktime.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (heap-based buffer overread and application crash) via a crafted mp4 file. CVE ID: CVE-2017-9128	com/exploit 2148/	A-LIB- LIBQU- 210617/ 122
Libquicktime					
Libquicktime			MsWrd1Parser::readFootnoteCo rrespondance function in lib/MsWrd1Parser.cxx. CVE ID: CVE-2017-9433		
Overflow	04-06-2017	7.5	Document Liberation Project libmwaw before 2017-04-08 has an out-of-bounds write caused by a heap-based buffer overflow related to the		A-LIB- LIBMW- 210617/ 121
Libmwaw					
DoS Libmwaw Proj	07-06-2017	4.3	attackers to cause a denial of service (SIGSEGV).	os://bugzill edhat.com/s v_bug.cgi?id 291299	A-LIB- LIBDW- 210617/ 120
Libdwarf Proje <i>Libdwarf</i>	ect				
				n/product_ urity/LEN- 149	210617/ 119
Execute Code	04-06-2017	7.2	version 4, a user with local Gain t.len	os://suppor novo.com/u	A-LEN- LENOV-

DoS 1	et		attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted mp4 file. CVE ID: CVE-2017-9122	s/42148/	120
			service (infinite loop and CPU consumption) via a crafted mp4 file.	S/42148/	120
	12-06-2017	7.1	The quicktime_read_moov function in moov.c in libquicktime 1.2.4 allows remote	https://www.e xploit- db.com/exploit	A-LIB- LIBQU- 210617/ 128
DoS 1	12-06-2017	4.3	The lqt_frame_duration function in lqt_quicktime.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted mp4 file. CVE ID: CVE-2017-9123	https://www.e xploit- db.com/exploit s/42148/	A-LIB- LIBQU- 210617/ 127
DoS 1	12-06-2017	4.3	The quicktime_match_32 function in util.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted mp4 file. CVE ID: CVE-2017-9124	https://www.e xploit- db.com/exploit s/42148/	A-LIB- LIBQU- 210617/ 126
DoS Overflow 1	12-06-2017	4.3	The lqt_frame_duration function in lqt_quicktime.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (heap-based buffer overread) via a crafted mp4 file. CVE ID: CVE-2017-9125	https://www.e xploit- db.com/exploit s/42148/	A-LIB- LIBQU- 210617/ 125
DoS Overflow 1	12-06-2017	4.3	via a crafted mp4 file. CVE ID: CVE-2017-9127 The quicktime_read_dref_table function in dref.c in libquicktime 1.2.4 allows remote attackers to cause a denial of service (heapbased buffer overflow and application crash) via a crafted mp4 file. CVE ID: CVE-2017-9126	https://www.e xploit- db.com/exploit s/42148/	A-LIB- LIBQU- 210617/ 124

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

Vulnerability Type(s):

 $DoS\text{-} Denial \ of \ Service; \ CSRF\text{-} Cross \ Site \ Request \ Forgery; \ XSS\text{-} Cross \ Site \ Scripting; \ Sql\text{-} SQL \ Injection; \ NA: \ Not \ Applicable$

Overflow Libstaroffice Pr	12-06-2017	6.8	In libsndfile version 1.0.28, an error in the "aiff_read_chanmap()" function (aiff.c) can be exploited to cause an out-of-bounds read memory access via a specially crafted AIFF file. CVE ID: CVE-2017-6892	https://github. com/erikd/libs ndfile/commit /f833c53cb59 6e9e1792949f 762e0b336618 22748	A-LIB- LIBSN- 210617/ 129
Libstar office	loject				
Overflow	04-06-2017	7.5	Document Liberation Project libstaroffice before 2017-04-07 has an out-of-bounds write caused by a stack-based buffer overflow related to the DatabaseName::read function in lib/StarWriterStruct.cxx. CVE ID: CVE-2017-9432	NA	A-LIB- LIBST- 210617/ 130
Libtiff					
Libtiff		1			T
DoS; Overflow	02-06-2017	4.3	In LibTIFF 4.0.7, a memory leak vulnerability was found in the function OJPEGReadHeaderInfoSecTables QTable in tif_ojpeg.c, which allows attackers to cause a denial of service via a crafted file. CVE ID: CVE-2017-9404	http://bugzilla. maptools.org/s how_bug.cgi?id =2688	A-LIB- LIBTI- 210617/ 131
DoS; Overflow	02-06-2017	4.3	In LibTIFF 4.0.7, a memory leak vulnerability was found in the function TIFFReadDirEntryLong8Array in tif_dirread.c, which allows attackers to cause a denial of service via a crafted file. CVE ID: CVE-2017-9403	http://bugzilla. maptools.org/s how_bug.cgi?id =2689	A-LIB- LIBTI- 210617/ 132
Markdown On	Save Improved	l Projec			
Markdown On S	Save Improved				
XSS	01-06-2017	4.3	The Markdown on Save Improved plugin 2.5 for WordPress has a stored XSS vulnerability in the content of a post.	http://lncken. cn/?p=279	A-MAR- MARKD- 210617/ 133
CV Scoring Scale (CVSS	5)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-10
Vulnerability Type(s):		iest Forger	y; XSS- Cross Site Scripting; Sql- SQL Injection; NA:	Not Applicable	

			CVE ID: CVE-2017-9337							
Markdown-it P	roject									
Markdown-it										
NA	07-06-2017	5	markdown-it before 4.1.0 does not block data: URLs. CVE ID: CVE-2015-3295	https://githu b.com/markd own- it/markdown- it/commit/f7 6d3beb46abd 121892a2e2e 5c78376354c 214e3	A-MAR- MARKD- 210617/ 134					
Mercurial										
Mercurial										
Execute Code	06-06-2017	9	In Mercurial before 4.1.3, "hg servestdio" allows remote authenticated users to launch the Python debugger, and consequently execute arbitrary code, by usingdebugger as a repository name. CVE ID: CVE-2017-9462	https://bugs. debian.org/86 1243	A-MER- MERCU- 210617/ 135					
Microsoft										
Excel;Office										
Execute Code	14-06-2017	9.3	A remote code execution vulnerability exists in Microsoft Office when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-8509, CVE-2017-8511, CVE-2017-8512, CVE-2017-0260, and CVE-2017-8506. CVE ID: CVE-2017-8510 E Web Apps; Office Web Apps Server	https://portal .msrc.microso ft.com/en- US/security- guidance/adv isory/CVE- 2017-8510	A-MIC- EXCEL- 210617/ 136					
Server;Word;Wo	•	ск;Ојјісе	e web Apps;OJJICE web Apps Server	;onenote;snare _[point					
Execute Code	14-06-2017	9.3	A remote code execution vulnerability exists in Microsoft Office when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This	https://portal .msrc.microso ft.com/en- US/security- guidance/adv isory/CVE-	A-MIC- OFFIC- 210617/ 137					
CV Scoring Scale (CVSS) Vulnerability Type(s): DoS- Denial of Service:		0-1	1-2 2-3 3-4 4-5 5-6 y; XSS- Cross Site Scripting; Sql- SQL Injection; NA: N		9-10					

Office: Office O	alino Sorvor: A	ffice We	CVE ID is unique from CVE-2017-8510, CVE-2017-8511, CVE-2017-8512, CVE-2017-0260, and CVE-2017-8506. CVE ID: CVE-2017-8509 b Apps; Office Web Apps Server; Po	2017-8509	ac:
Sharepoint Ser		jice we	o Apps, Office web Apps server, 1 c	werpoint for M	ис,
Execute Code	14-06-2017	9.3	A remote code execution vulnerability exists in Microsoft Office when the software fails to properly handle objects in memory, aka "Office Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-8509, CVE-2017-8510, CVE-2017-8511, CVE-2017-0260, and CVE-2017-8506. CVE ID: CVE-2017-8512	https://portal .msrc.microso ft.com/en- US/security- guidance/adv isory/CVE- 2017-8512	A-MIC- OFFIC- 210617/ 138
Milton					
Webdav					_
NA	07-06-2017	7.5	XML External Entity (XXE) vulnerability in Milton Webdav before 2.7.0.3. CVE ID: CVE-2015-7326	https://githu b.com/miltoni o/milton2/co mmit/b5851c	A-MIL- WEBDA- 210617/ 139
Multi Feed Rea	der Project				
Multi Feed Read					
Execute Code; Sql	09-06-2017	6.5	SQL injection vulnerability in the Multi Feed Reader prior to version 2.2.4 allows authenticated attackers to execute arbitrary SQL commands via unspecified vectors. CVE ID: CVE-2017-2195	https://word press.org/plu gins/multi- feed- reader/#deve lopers	A-MUL- MULTI- 210617/ 140
Opa-ff Project;	Opa-fm Projec	t			
Opa-ff/Opa-fm					
NA	07-06-2017	9.3	Race conditions in opa-fm before 10.4.0.0.196 and opa-ff before 10.4.0.0.197. CVE ID: CVE-2015-5232	https://githu b.com/01org/ opa- fm/commit/c 5759e7b76f5 bf844be6c66 41cc1b356bb	A-OPA- OPA-F- 210617/ 141
CV Scoring Scale (CVSS		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-10
Vulnerability Type(s): DoS- Denial of Service;		iest Forger	y; XSS- Cross Site Scripting; Sql- SQL Injection; NA:	Not Applicable	

								c838	69			
Openbravo												
Openbravo Erp)											
Sql	05-06-2017	6.5	Openbravo Business Suite 3.0 is affected by SQL injection. This vulnerability could allow remote authenticated attackers to inject arbitrary SQL code. CVE ID: CVE-2017-9437				https://www. wizlynxgroup. com/security- research- advisories/vu ln/WLX- 2017-005			A-OF OPE 2106 142	NB-	
Open-emr												
Openemr												
Execute Code	02-06-2017	6.5	OpenEMR 5.0.0 and prior allows low-Gain Privileges users to upload files of dangerous types which can result in arbitrary code execution within the context of the vulnerable application. CVE ID: CVE-2017-9380				https://www. wizlynxgroup. com/security- research- advisories/vu ln/WLX- 2017-002			A-OPE- OPENE- 210617/ 143		
Open-xchange												
Open-xchange	Appsuite;Open	-xchang	e Serve	er								
XSS	08-06-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Open-Xchange Server 6 and OX AppSuite before 7.4.2-rev43, 7.6.0-rev38, and 7.6.1-rev21. CVE ID: CVE-2015-1588					NA			A-OF OPE 2106 144	N
Personify												
Personify360 E	-business											
NA	07-06-2017	5	An issue was discovered in Personify360 e-Business 7.5.2 through 7.6.1. When going to the /TabId/275 URI, while creating a new role, a list of database tables and their columns is available. CVE ID: CVE-2017-7314				https://amsw oes.wordpres s.com/2017/ 06/06/CVE- 2017-7314- dump- personify- database- schema-33/		es /	A-PER- PERSO- 210617/ 145		
Gain Information	07-06-2017	5	An issue was discovered in Personify360 e-Business 7.5.2 through 7.6.1. When going to the /TabId/275 URI, it is possible to read any customer name, master					https://amsw oes.wordpres s.com/2017/ 06/06/CVE- 2017-7313-		sw es /	A-PER- PERSO- 210617/ 146	
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	9	9-10
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable												

			In other search for system - required	er Id, and en words, any or users/cu no authen d. CVE-2017	one car stomer tication	n s in the	custo data-		/	
NA	07-06-2017	7.5	An issue Personid through /TabId/ a vendor vendor a usernan	was discoving was discoving was discovered with the was discovered with the was discovered with the was discovered was discovered with the was discove	vered in siness 7 on going nyone carread e (inclustrate)	.5.2 to the an add xisting ding	https oes.w s.con 06/0	s://amsv vordpre n/2017/ 6/first- post/	w A s P ' 2	-PER- ERSO- 10617/ 47
Pivotx										
Pivotx										
XSS	06-06-2017	4.3	modules PivotX 2 allowing quotes i	orty_self fur s/module_s s.3.11 misha g XSS via ve n the self Si CVE-2017	marty.p andles ti ctors in marty ta	hp in he URI, volving	eforg pivot	og/code	/ P 2	-PIV- IVOT- 10617/ 48
Piwigo										
Piwigo										
NA	14-06-2017	5.8	present probably remote a to arbitr conduct identifica affected "redirect validate	redirect vom Piwigo 2 y prior verse attackers to phishing attation.php of the by this issuit parameted. CVE-2017	.9 and sions, all redirectes and ttacks. To componential the er is not	lowing ct users The ent is	NA		P 2	-PIW- IWIG- 10617/ 49
Postgresql										
Postgresql										
NA	06-06-2017	5	does not	SQL PL/Java t honor acca jects. CVE-2016	ess cont		ithub	s://tada. o.io/plja easenot il	v P e 2	-POS- OSTG- 10617/ 50
Pulpproject			U. 2.121	J. 2 2010	2.00		Jiiii			
Pulp										
CV Scoring Scale (CV	/SS)	0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s DoS- Denial of Servi	s): ce; CSRF-Cross Site Requ	uest Forger	y; XSS- Cross	Site Scripting; S	ql- SQL Inje	ection; NA:	Not Appli	cable		

	(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Nexpose NA	06-06-2017	6.8	Rapid applia 2017 algori other result ALL a releva make vulne	To Nexpances sladoes no thing for the contract of the contract	ose had nipped of speciant fundable back to ms supped stallation of a range o	before ify desir exchang excions. o allow ported OpenSS	June red ge and As a ing by the H and	unity om/ ty/n log/2 31/r 13-n hard appl ssh-e obso	s://com y.rapid7 commur expose/ 2017/05 7-2017- expose- ware- iance- enabled- olete- rithms-	.c N ni 2 b 1	1-RAP- IEXPO- 110617/ 54
Rapid7											
DoS	08-06-2017	4.3	libr/c 1.5.0 cause after- via a	onfig/o allows i a denia	config.c cemote al of sea d appli DEX fil		re2 ers to se-	b.com/rad/mmi/74b2/64fe	s://githum/radar are2/co t/f85bco 2a2256a 796351 71e1060	re R 2 6 1 3 b	A-RAD- RADAR- 210617/ 53
Radare2	08-06-2017	4.2	Tha	confic	got for	ation :-		http://	o. / /a:+ls-	, ,	DAD
Radare Pro	ject										
Qemu Qemu DoS	01-06-2017	4.9	Memo virtio hw/d (aka (guest servio via a l "VIRT T:" co	ory leak _gpu_se isplay/ Quick E OS use ce (men arge nu	in the et_scanding virtio-generate canding to canding to canding the canding the canding to canding the cand	out fung gpu.c in r) allov use a d onsump of _SET_S(vs local enial of tion)	mu.g mu.g mit;l d7e2 8739	://git.qe org/?p=c git;a=cor n=dd248 204ee8a 914e02b 6e8f1b86	де С n 2 Ве 1 1 08	A-QEM- QEMU- 110617/ 52
				D: CVE			abic.				
NA	08-06-2017	5	befor Gain l etc/p	e 2.8.3 v Privileg ki/pulp	writes esate k /consu	i.py in I consum ceys to imer/co d-reada	onsum	_	s://pulp o/issues 4	s/ P 2	A-PUL- PULP- 10617/ 51

			CVE ID: CVE-2017-5243	5243	
Rarlab					
RAR					
Directory Traversal	04-06-2017	4.3	Directory Traversal exists in RAR 4.x and 5.x because an unpack operation follows any symlinks, including symlinks contained in the archive. This allows remote attackers to write to arbitrary files via a crafted archive. CVE ID: CVE-2014-9983	https://bugs. debian.org/cg i- bin/bugrepor t.cgi?bug=774 172	A-RAR- RAR- 210617/ 155
Redhat					
Cloudforms					
Execute Code	08-06-2017	6.5	ManageIQ in CloudForms before 4.1 allows remote authenticated users to execute arbitrary code. CVE ID: CVE-2016-4471	https://bugzil la.redhat.com /show_bug.cg i?id=1340763	A-RED- CLOUD- 210617/ 156
Cloudforms Ma	nagement Eng	ine			
NA	08-06-2017	5	CloudForms Management Engine before 5.8 includes a default SSL/TLS certificate. CVE ID: CVE-2016-4457	https://bugzil la.redhat.com /show_bug.cg i?id=1341308	A-RED- CLOUD- 210617/ 157
Satellite					
NA	07-06-2017	6.5	Red Hat Satellite 6 allows remote authenticated users with Gain Privileges access on a content host to authenticate to the capsule broker or server broker. CVE ID: CVE-2015-5202	https://bugzil la.redhat.com /show_bug.cg i?id=1253884	A-RED- SATEL- 210617/ 158
Saat					
Netizen					
Gain Privileges	09-06-2017	6.8	Untrusted search path vulnerability in the installer of SaAT Netizen ver.1.2.10.510 and earlier allows an attacker to gain Gain Privileges via a Trojan horse DLL in an unspecified directory. CVE ID: CVE-2017-2206	https://www. saat.jp/infor mation/netize n/2017/0531 _security_upd ate_info.php	A-SAA- NETIZ- 210617/ 159
Personal					
Gain Privileges	09-06-2017	6.8	Untrusted search path vulnerability in the installer of SaAT Personal ver.1.0.10.272 and	https://www. saat.jp/infor mation/perso	A-SAA- PERSO- 210617/
CV Scoring Scale (CVSS Vulnerability Type(s):)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-10

 $DoS\text{-} Denial \ of \ Service; \ CSRF\text{-} Cross \ Site \ Request \ Forgery; \ XSS\text{-} Cross \ Site \ Scripting; \ Sql\text{-} SQL \ Injection; \ NA: \ Not \ Applicable$

Samsung Syncthru 6	6-06-2017 1-06-2017	7.8	4.5.x be service (fd_ope with his consum handling CVE ID Multiple vulnerary SyncTheremote arbitrary parameters	efore 4.5.6 vulnerabilen_atomic igh CPU usanption) due gedangling: CVE-201 e directoryabilities in aru 6 before attackers	nfinite loop age and me e to wrongly symlinks. 7-9461 v traversal Samsung e 1.0 allow to delete unspecifie	nl of p mory ly		s://bugs an.org/8	36	A-SAM- SAMBA- 210617/ 161 A-SAM- SYNCT- 210617/ 162
Samsung Syncthru 6 Execute Code; Directory			4.5.x be service (fd_ope with his consum handling CVE ID Multiple vulnerary SyncTheremote arbitrary parameters	efore 4.5.6 vulnerabilen_atomic is gh CPU usanption) due in g dangling : CVE-201 e directory abilities in aru 6 before attackers ry files via	has a deniality nfinite loop age and me to wrongly symlinks. 7-9461 Variation Yaversal Samsung to delete unspecifie	nl of p mory ly	debia 4291	an.org/8	36	SAMBA- 210617/ 161 A-SAM- SYNCT- 210617/
Samsung Syncthru 6 Execute Code; Directory			4.5.x be service (fd_ope with his consum handling CVE ID Multiple vulnerary SyncTheremote arbitrary parameters	efore 4.5.6 vulnerabilen_atomic is gh CPU usanption) due in g dangling : CVE-201 e directory abilities in aru 6 before attackers ry files via	has a deniality nfinite loop age and me to wrongly symlinks. 7-9461 Variation Yaversal Samsung to delete unspecifie	nl of p mory ly	debia 4291	an.org/8	36	SAMBA- 210617/ 161 A-SAM- SYNCT- 210617/
Syncthru 6 Execute Code; 01 Directory	1-06-2017	10	vulnera SyncTh remote arbitra parame	abilities in ru 6 before attackers ry files via	Samsung e 1.0 allow to delete unspecifie	NA			SYNCT- 210617/	
Execute Code; 01 Directory	1-06-2017	10	vulnera SyncTh remote arbitra parame	abilities in ru 6 before attackers ry files via	Samsung e 1.0 allow to delete unspecifie		NA			SYNCT- 210617/
Directory	1-06-2017	10	vulnera SyncTh remote arbitra parame	abilities in ru 6 before attackers ry files via	Samsung e 1.0 allow to delete unspecifie		NA			SYNCT- 210617/
			upload, arbitra Privileg parame upload fileuplo upload upload	ry code wit gesileges vieters to (3) Cloning.htm ad.html, (!	iver or (2) r or to exect th SYSTEM ia unspecif ml, (4) 5) html, or (6)	cute Gain ied				
Schneider-electric	<u> </u>									
Somachine							T .			
Overflow 07	7-06-2017	4.6	exists in executa Schneid HVAC v M171/I	n Program able AlTrac	roller.	chne elect n/do docu	//www ider- ric.com, wnload ment/S 017-12	/e / E	A-SCH- SOMAC- 210617/ 163	
Execute Code 07	7-06-2017	6.8	A DLL I	Hijacking v	ulnerabilit	y in	http:	//www	.s	A-SCH-
CV Scoring Scale (CVSS)		0-1	1-2	2-3 3-4	4-5		6-7	7-8	8-9 9-	

		the programming software Schneider Electric's SoMack HVAC v2.1.0 allows a remo- attacker to execute arbitrar on the targeted system. The							eider- tric.com ownload	n/e d/	SOMAC- 210617/ 164
			on th vulne impr		ted syst exists ading of	em. The due to t f a DLL.	e the		1ment/S 2017-12		
Simple Keitai C	hat Project		CVE	ID: CVE	-201/-	7900					
Simple Keitai C	•										
XSS	09-06-2017	4.3	in Sir earlie inject HTM	s-site sc nple ke er allow t arbitra L via un ID: CVE	itai cha s remo ary web specifi	t 2.0 an te attac script ed vecto	d kers to or	NA			A-SIM- SIMPL- 210617/ 165
Skygroup											
Skysea Client Vi	iew										
Execute Code	09-06-2017	10	Ver.1 remo in pro the T mana	EA Clie 1.221.0 te code ocessing CP connagement	3 and e execut g authe nection t conso	earlier a ion via nticatio with th le progi	a flaw on on e	skyg	/17030	/s	A-SKY- SKYSE- 210617/ 166
Slideshow Proj	ect										
Slideshow											
info	08-06-2017	5	The SlideshowPluginSlideshowStyles heet::loadStylesheetByAJAX function in the Slideshow plugin 2.2.8 through 2.2.21 for Wordpress allows remote attackers to read arbitrary Wordpress option values. CVE ID: CVE-2015-3634					https://githu b.com/Boonst ra/Slideshow /commit/cac5 05e593cbe70 a4d8af5b639f 5385d4cc7aa 04			A-SLI- SLIDE- 210617/ 167
Soffid											
Evacuta Codo	02.06.2017	7 -	11	roks d T		alie ar i i	a isa	1-1-	. / /		A COE
Execute Code	UZ-U6-ZU1/	02-06-2017 7.5 Untrusted Java serialization in Soffid IAM console before 1.7.5 allows remote attackers to achieve arbitrary remote code execution via a crafted						offid urity	sory1-	ec	A-SOF- IAM- 210617/ 168
							5-6	6-7			

			authentication request.		
Canhag			CVE ID: CVE-2017-9363		
Sophos Web Appliance					
Web Applianc XSS	08-06-2017	4.3	The Sophos Web Appliance before 4.3.2 has XSS in the FTP redirect page, aka NSWA-1342. CVE ID: CVE-2017-9523	http://swa.so phos.com/rn/ swa/concepts /ReleaseNote s_4.3.2.html	A-SOP- WEB A- 210617/ 169
Spiffy					
Spiffy					
Directory Traversal	07-06-2017	5	Directory traversal vulnerability in Spiffy before 5.4. CVE ID: CVE-2015-8235	http://code.ca ll-cc.org/cgi- bin/gitweb.cgi ?p=chicken- core.git;a=co mmit;h=edd4 926bb4f4c97 760a0e03b0d 0e8210398fe 967	A-SPI- SPIFF- 210617/ 170
Subsonic					
Subsonic					
NA	07-06-2017	4.3	XML external entity (XXE) vulnerability in the import playlist feature in Subsonic 6.1.1 might allow remote attackers to conduct server-side request forgery (SSRF) attacks via a crafted XSPF playlist file. CVE ID: CVE-2017-9355	NA	A-SUB- SUBSO- 210617/ 171
Sunnythemes					
Spiffy Calenda	ır			_	
XSS	05-06-2017	4.3	Cross site scripting (XSS) vulnerability in the Spiffy Calendar plugin before 3.3.0 for WordPress allows remote attackers to inject arbitrary JavaScript via the yr parameter. CVE ID: CVE-2017-9420	NA	A-SUN- SPIFF- 210617/ 172
Teampass					
Teampass					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s):										
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

Sql	05-06-2017	7.5	TeamPass by vulnerable users.queri	to a SQL es.php.	injecti		.com passi Pass,	s://gith /nilstea net/Tea /blob/i /change	am am na	A-TEA TEA 2106 173	MP-
Todd Miller											
Sudo							Τ,				
Execute Code	05-06-2017	6.9	Todd Miller and earlier input valida spaces) in t get_process resulting in disclosure a execution. CVE ID: CV	is vulne ntion (en he _ttynam informa and com	rable to nbedde ne() fun ntion mand	an d ction	sudo	s://ww .ws/ale ux_tty.l	ert	A-T(SUD) 2106 174	
Execute Code	05-06-2017	7.2	Todd Miller 1.8.20p1 and to an input newlines) in get_process resulting in disclosure a execution. CVE ID: CV	d earlie validation the _ttynam informa	r is vulton (eml ee() fun ation mand	nerable pedded ction	sudo	s://ww .ws/ale ux_tty.l	ert	A-TO SUD 2106 175	
Torproject			0.2.2.0.								
Tor											
DoS	09-06-2017	5	The hidden before 0.3.0 service (ass daemon exi connection ell function on a rendez CVE ID: CV	.8 allow ertion fa t) in the _edge_pi via a BE vous cir	s a den ailure a cocess_ GIN_DI cuit.	ial of nd relay_c	.com ct/to t/56a e044 1c1e	s://gith /torpro r/comi a7c5bc 7203a4 e37de9 1dcd	oje mi 15 49	A-T(TOR 2106 176	-
DoS	09-06-2017	5	The hidden before 0.3.0 service (ass daemon exi relay_send_function via cell.	0.8 allow ertion fa t) in the end_cell	s a den ailure a _from_	ial of nd edge_	https://github .com/torproje ct/tor/commi t/79b59a2dfc b68897ee89d 98587d09e55 f07e68d7			A-TOR TOR 2106 177	-
CV Scoring Scale (CVSS)	0-1	1-2 2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10

			CVE ID: CVE-2017-0375		
Unisys					
Mobigate					
Gain Information	09-06-2017	4.3	The mobiGate App for Android version 2.2.1.2 and earlier and mobiGate App for iOS version 2.2.4.1 and earlier do not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. CVE ID: CVE-2016-7805	NA	A-UNI- MOBIG- 210617/ 178
Virustotal					
Yara					
DoS DoS; Overflow;	05-06-2017	5.8	libyara/re.c in the regexp module in YARA 3.5.0 allows remote attackers to cause a denial of service (stack consumption) via a crafted rule (involving hex strings) that is mishandled in the _yr_re_emit function, a different vulnerability than CVE-2017-9304. CVE ID: CVE-2017-9438 The yr_arena_write_data function	https://github .com/VirusTo tal/yara/issue s/674	A-VIR- YARA- 210617/ 179
Gain Information			in YARA 3.6.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) or obtain sensitive information from process memory via a crafted file that is mishandled in the yr_re_fast_exec function in libyara/re.c and the _yr_scan_match_callback function in libyara/scan.c. CVE ID: CVE-2017-9465	.com/VirusTo tal/yara/com mit/992480c 30f75943e9cd 6245bb2015c 7737f9b661	YARA- 210617/ 180
Vmware					
Fusion;Worksta	ition				
Execute Code; Overflow	08-06-2017	7.5	The drag-and-drop (DnD) function in VMware Workstation	https://www. vmware.com/	A-VMW- FUSIO-
CV Scoring Scale (CVSS))	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-10
Vulnerability Type(s): DoS- Denial of Service;	CSRF-Cross Site Requ	iest Forgery	y; XSS- Cross Site Scripting; Sql- SQL Injection; NA: I	Not Applicable	

Horizon View; U	Inified Access (Gateway	12.x before version 12.5.4 and Fusion 8.x before version 8.5.5 has an out-of-bounds memory access vulnerability. This may allow a guest to execute code on the operating system that runs Workstation or Fusion. CVE ID: CVE-2017-4901 security/adviories/VMSA- 2017- 0005.html	s 210617/ 181
Execute Code; Overflow	08-06-2017	7.5	VMware Unified Access Gateway (2.5.x, 2.7.x, 2.8.x prior to 2.8.1) and Horizon View (7.x prior to 7.1.0, 6.x prior to 6.2.4) contain a heap buffer-overflow vulnerability which may allow a remote attacker to execute code on the security gateway. CVE ID: CVE-2017-4907	HORIZ-
Horizon View; V DoS; Execute	08-06-2017	6.9	VMware Workstation (12.x prior http://www.	A-VMW-
Code; Overflow	00.06.2017		to 12.5.3) and Horizon View Client (4.x prior to 4.4.0) contain an integer-overflow vulnerability in the True Type Font parser in the TPView.dll. On Workstation, this may allow a guest to execute code or perform a Denial of Service on the Windows OS that runs Workstation. In the case of a Horizon View Client, this may allow a View desktop to execute code or perform a Denial of Service on the Windows OS that runs the Horizon View Client. Exploitation is only possible if virtual printing has been enabled. This feature is not enabled by default on Workstation but it is enabled by default on Horizon View. CVE ID: CVE-2017-4913	210617/183
DoS Execute Code	08-06-2017	6.9	VMware Workstation (12.x prior to 12.5.3) and Horizon View http://www.	
			Client (4.x prior to 4.4.0) contain ecurity/advis	210617/
CV Scoring Scale (CVSS)		0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8	8-9 9-10

DoS Execute 08-06-2017 6.9 VMware Workstation (12.x prior http://www.v A-VMW-	Code	08-06-2017	6.9	(TTF) On W guest a Der Wind Work Horiz allow code Servi runs Explo virtus This i defau enabl View CVE I VMw to 12 Clien multi vulne parse Work guest a Der Wind Work Horiz allow code Servi runs Explo virtus This i defau enabl View CVE I	parsendorkstand of Schools of Sch	r in the tion, this cute cook of that rule to the wellien of the w	s may a de or per on the ins case of the period of the possib been enabled the ins case of the	r.dll. allow a allow a perform a hay ecute for that ent. le if habled. by the it is zon a prior wontain ite on wall allow a perform a hay ecute for the inabled. by the it is zon.	http: mwa ecuri ories 2017 0008	3.html //www ire.com ity/adv s/VMSA 7- 3.html	/s is i-	A-VMV HORIZ 21061 185	7/
UV Scoring Scale (UVSS)	CV Scoring Scale (CVSS)	00 00-2017											

			CVE I	D: CVE	-2017	4909							
DoS Execute Code Overflow	08-06-2017	6.9	to 12 Clien multi vulne parse Work guest a Den Wind Work Horiz allow code Servi runs Explo virtua This d defau enabl	15.3) and t (4.x proposed to execute the contraction of Station of Station of Station of Station of the Horotation of Station of Station of Station of the Horotation of Station	nd Horizarior to a possible to the possible to the control of the possible to	case of t, this nop to ex Oenial o dows Os ew Clie been e enabled tion but	ontain low 0 n w a erform a a a a b b b b b c t i t i s c d d d d d d d d d d d d d d d d d d	mwa ecuri ories 2017	//www. re.com/ ity/advis /VMSA- '- 8.html	s 1	A-VMW- HORIZ- 210617/ 188		
Vsphere Data P	Protection												
Gain Information	07-06-2017	5	(VDP locall crede encry plain obtai) 6.1.x, y store entials u ption. ' text cre	6.0.x, 5 s vCent using re This iss edential		d 5.5.x er e	mwa ecuri ories 2017	//www. re.com/ ity/advis //VMSA- /-).html	s S	A-VMW- VSPHE- 210617/ 189		
Execute Code	07-06-2017	7.5	(VDP conta Explo allow execu appli) 6.1.x, nins a de pitation a remo ute com	6.0.x, 5 eseriali of this ote atta mands	on the	d 5.5.x ssue.	mwa ecuri ories 2017	//www. re.com/ ty/advis //WSA- /-).html	S Z	A-VMW- VSPHE- 210617/ 190		
Workstation Pl	ayer; Workstat	tion Pro						1					
NA	07-06-2017	6.9	VMware Workstation Pro/Player 12.x before 12.5.3 contains a DLL						http://www.v mware.com/s		A-VMW- WORKS-		
CV Scoring Scale (CVSS		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
	CV Scoring Scale (CVSS) Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable												

			loading vulnerability that occurs due to the "vmware-vmx" process loading DLLs from a path defined in the local environment-variable. Successful exploitation of this issue may allow normal users to escalate Gain Privileges to System in the host machine where VMware Workstation is installed. CVE ID: CVE-2017-4898	ecurity/advis ories/VMSA- 2017- 0003.html	210617/ 191
Websitebaker					
Websitebaker XSS	02-06-2017	4.3	WebsiteBaker v2.10.0 has a stored XSS vulnerability in /account/details.php. CVE ID: CVE-2017-9361	https://jgj212 .blogspot.tw/ 2017/05/a- stored-xss- vulnerability-	A-WEB- WEBSI- 210617/ 192
Sql	02-06-2017	7.5	WebsiteBaker v2.10.0 has SQL injection vulnerability in /account/details.php. CVE ID: CVE-2017-9360	in.html https://jgj212 .blogspot.tw/ 2017/05/a- sql-injection- vulnerability- in.html	A-WEB- WEBSI- 210617/ 193
Winsparkle					
Winsparkle					
Execute Code	09-06-2017	6.8	Untrusted search path vulnerability in WinSparkle versions prior to 0.5.3 allows remote attackers to execute arbitrary code via a specially crafted executable file in an unspecified directory. CVE ID: CVE-2016-7838	https://www. wireshark.org /news/20161 214.html	A-WIN- WINSP- 210617/ 194
Wireshark					
Wireshark NA	14-06-2017	4.3	In Wireshark 2.2.7, overly deep mp4 chunks may cause stack exhaustion (uncontrolled recursion) in the dissect_mp4_box function in epan/dissectors/file-mp4.c. CVE ID: CVE-2017-9616	https://bugs. wireshark.org /bugzilla/sho w_bug.cgi?id= 13777	A-WIR- WIRES- 210617/ 195
CV Scoring Scale (CVSS	5)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-10

CV Scoring Scale (C	vss)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
NA	02-06-2017	5		ireshar		to 2.2.6	and	NA		A	-WIR-
NA	02-06-2017	5	2.0.0 L2CA zero. epan by va	to 2.0.1 P disse This w /dissec lidating	Bluetoould divessed in the contract of the con	NA		W 2:	-WIR- /IRES- 10617/ 01		
NA	02-06-2017	5	ROS of NULI was a epan t-ros OID.	ireshar dissecto pointe ddress dissec templa	or could er deref ed in tors/as ite.c by	l crash erence n1/ros validat	with a . This	NA		W 2:	-WIR- /IRES- 10617/ 00
Overflow	02-06-2017	5	DOF end of address epan valid.	of a buffessed in dissec ating a	or could fer. This n tors/pa size val -2017	d read _l s was acket-d ue. 9348	oast the	NA		W 2 1	-WIR- /IRES- 10617/ 99
Overflow	02-06-2017	5	2.0.0 disse of a b epan by ex Ident		12, the 1 uld rea This wa tors/pa g the Vo	OHCP d past t s addre acket-b endor (efully.	the end essed in ootp.c	NA		W 2:	-WIR- /IRES- 10617/ 98
NA	02-06-2017	5	IPv6 was a epan valid	ireshar dissect address /dissec ating ar	or coul ed in tors/pa n IPv6 a	d crash ncket-ip nddress	. This	NA		W 2:	-WIR- /IRES- 10617/ 97
NA	02-06-2017	5	2.0.0 disse addre epan by va	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the RGMP dissector could crash. This was addressed in epan/dissectors/packet-rgmp.c by validating an IPv4 address. CVE ID: CVE-2017-9354						W 2	-WIR- /IRES- 10617/ 96

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
NA	02-06-2017	7.8	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the SoulSeek dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-slsk.c by making loop bounds more					NA		2	A-WIR- WIRES- 210617/ 207
NA	02-06-2017	7.8	2.0.0 disse This epan valid	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DICOM dissector has an infinite loop. This was addressed in epan/dissectors/packet-dcm.c by validating a length value. CVE ID: CVE-2017-9349				NA		2	A-WIR- WIRES- 210617/ 206
NA	02-06-2017	7.8	2.0.0 disse syste addre epan open negar	to 2.0.1 to 2.0.1 ctor commem m mem essed in /dissective safety.ctive len	2, the ould crashory. The tors/past character is the char	openSAsh or ex his was acket- cking fo	FETY haust or a	NA			A-WIR- WIRES- 210617/ 205
NA	02-06-2017	7.8	2.0.0 disse loop. epan ensur canno	to 2.0.1 to 2.0.1 ctor con This w /dissec ring tha ot occur ID: CVE	2, the land go it as addrates addrates addrates addrates addrates and addrates addra	Bazaar nto an i ressed i acket-ba wards p	infinite n zr.c by arsing	NA			A-WIR- WIRES- 210617/ 204
NA	14-06-2017	5	In Windows DAAI exhaurecur disse epan the D	ID: CVE ireshar data n ustion (rsion) in ct_daap	k 2.2.7, hay cau funcont the o_one_t tors/pa	deeply se stack rolled ag funct acket-da	nested k	wire: /bug	s://bug shark.o zilla/sh ig.cgi?io	rg V	A-WIR- WIRES- 210617/ 203
			disse point epan by va	to 2.0.1 ctor mi cer. This /dissec	suses as was a tors/pagan IPv	NULL ddresse acket-m v4 addr	snip.c			2	WIRES- 210617/ 202

CV Scoring Scale (CVS		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
DoS	07-06-2017	4.3	In ytnef 1.9.2, the TNEFFillMapi function in lib/ytnef.c allows remote attackers to cause a denial of service (memory consumption) via a crafted file. CVE ID: CVE-2017-9473	https://blogs. gentoo.org/ag o/2017/05/2 4/ytnef- memory- allocation- failure-in- tneffillmapi- ytnef-c/	A-YTN- YTNEF- 210617/ 212
Ytnef DoS Overflow	07-06-2017	4.3	In ytnef 1.9.2, the DecompressRTF function in lib/ytnef.c allows remote attackers to cause a denial of service (heap-based buffer over- read and application crash) via a crafted file. CVE ID: CVE-2017-9474	https://blogs. gentoo.org/ag o/2017/05/2 4/ytnef-heap- based-buffer- overflow-in- decompressrt f-ytnef-c/	A-YTN- YTNEF- 210617/ 211
Ytnef Project					
XSS	01-06-2017	4.3	The WP Editor.MD plugin 1.6 for WordPress has a stored XSS vulnerability in the content of a post. CVE ID: CVE-2017-9336	http://lncken. cn/?p=258	A-WP - WP ED- 210617/ 210
Wp Editor.md Wp Editor.md	Project				
XSS	07-06-2017	4.3	Cross-site scripting (XSS) vulnerability in the WordPress Backup to Dropbox plugin before 4.1 for WordPress. CVE ID: CVE-2014-9310	https://word press.org/plu gins/wordpre ss-backup-to- dropbox/	A-WOR- WORDP- 210617/ 209
Wordpress Ba	ckup To Dropbo	X			
Wordnross Ra	ckup To Dropb	ov Proj	pointers. CVE ID: CVE-2017-9345		
			could go into an infinite loop. This was addressed in epan/dissectors/packet-dns.c by trying to detect self-referencing		210617/ 208
NA	02-06-2017	7.8	CVE ID: CVE-2017-9346 In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DNS dissector	NA	A-WIR- WIRES-

4.3	In ytnef 1.9.2, the SwapDWord https://blogs. A-YTN-											
	function in lib/ytnef.c allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file. CVE ID: CVE-2017-9472 gentoo.org/ag o/2017/05/2 4/ytnef-heap- based-buffer- overflow-in- swapdword- ytnef-c/											
4.3	In ytnef 1.9.2, the SwapWord function in lib/ytnef.c allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file. CVE ID: CVE-2017-9471 In ytnef 1.9.2, the SwapWord gentoo.org/ag o/2017/05/2 4/ytnef-heap-based-buffer overflow-in-swapword-ytnef-c/											
4.3	In ytnef 1.9.2, the MAPIPrint function in lib/ytnef.c allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file. CVE ID: CVE-2017-9470 https://blogs. gentoo.org/ag o/2017/05/2 4/ytnef-null-pointer dereference-in-mapiprint-ytnef-c/											
7.5	SQL injection vulnerability in ZCMS 1.1. CVE ID: CVE-2015-7346 R-ZCM- ZCMS- 210617/ 216											
6.8	Cross-site request forgery (CSRF) vulnerability in la.redhat.com ZEND - Zend/Validator/Csrf in Zend /show_bug.cg i?id=1207781 217 217 217 217 217 217 217 217 217 21											
plicati	on/ Operating System (A/OS)											
<u> </u>	vell/GIT											
Ubuntu Linux/Debian Linux/Fedora/Leap/Git-shell												
6.5	git-shell in git before 2.4.12, 2.5.x https://kernel A-OS-before 2.5.6, 2.6.x before 2.6.7, googlesource. CAN-											
0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10											
	6.5											

			2.7.x before 2.7.5, 2.8.x before 2.8.5, 2.9.x before 2.9.4, 2.10.x before 2.10.3, 2.11.x before 2.11.2, and 2.12.x before 2.12.3 might allow remote authenticated users to gain Gain Privileges via a repository name that starts with a - (dash) character. CVE ID: CVE-2017-8386	com/pub/scm /git/git/+/3ec 804490a265f 4c418a32142 8c12f3f18b7e ff5	UBUNT- 210617/ 218
Fedoraproject:	 Novell:Opensu	se Proi	ect/Game-music-emu Project		
	<u> </u>		p;Suse Linux Enterprise Server;Sus	e Linux Enterpri	'se
Software Develo					
NA	06-06-2017	10	game-music-emu before 0.6.1 mishandles unspecified integer values. CVE ID: CVE-2016-9961	https://bugzil la.redhat.com /show_bug.cgi ?id=1405423	A-OS- FED- FEDOR- 210617/ 219
PHP/Suse					
PHP/Linux Ente	erprise Module	For We	b Scripting;Linux Enterprise Softw	are Developmen	t Kit
Execute Code	08-06-2017	7.5	/ext/phar/phar_object.c in PHP 7.0.7 and 5.6.x allows remote attackers to execute arbitrary code. NOTE: Introduced as part of an incomplete fix to CVE-2015-6833. CVE ID: CVE-2016-4473	https://bugzil la.redhat.com /show_bug.cg i?id=1347772	A-OS- PHP- PHP/L- 210617/ 220
Vmware/Vmwa) Pro		CVE ID: CVE-2016-4473		
<u> </u>		station l	Player;Workstation Pro		
Execute Code; Overflow	07-06-2017	7.2	VMware ESXi 6.5 without patch ESXi650-201703410-SG and 5.5 without patch ESXi550-201703401-SG; Workstation Pro / Player 12.x prior to 12.5.5; and Fusion Pro / Fusion 8.x prior to 8.5.6 have a Heap Buffer Overflow in SVGA. This issue may allow a guest to execute code on the host. CVE ID: CVE-2017-4902	http://www.v mware.com/s ecurity/advis ories/VMSA- 2017- 0006.html	A-OS- VMW- ESXI/- 210617/ 221
Esxi/Fusion;Wo	1			T	
DoS; Execute Code; Overflow	07-06-2017	7.2	The XHCI controller in VMware ESXi 6.5 without patch ESXi650-201703410-SG, 6.0 U3 without	http://www.v mware.com/s ecurity/advis	A-OS- VMW- ESXI/-
CV Scoring Scale (CVSS	<u> </u>	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-10
Vulnerability Type(s):		iest Forger	y; XSS- Cross Site Scripting; Sql- SQL Injection; NA: I	Not Applicable	

			natah	FCV:40	<u></u>	702401	_SC	orio	C /\/N/C A		210617/
Events C. J.	07.06.2047	7.0	6.0 U2 2017(patch and 5. 2017(/ Play Fusion 8.5.6 l usage guest The is Service CVE II	2 witho 03403-; ESXi60 .5 witho 03401-; er 12.x n Pro / has uni . This is to exect sue is n ce of the	ut pate SG, 6.0 00-201 out pat SG; Wo Fusior Fusior nitializ ssue m cute co reduce e guest -2017-	d to a D on ESX ·4904	600- hout 2-SG, i550- on Pro 5; and ior to mory v a ne host. eenial of	2017	5.html		210617/222
Execute Code Overflow	07-06-2017	7.2	ESXi6 witho 2017(patch 6.0 U1 2017(patch Works prior Fusion uninit in SV(guest	50-201 ut patc 03401- ESXi60 I witho 03402- ESXi55 station to 12.5 n 8.x probable GA. This	TO341 h ESXid SG, 6.0 00-201 ut pato SG, and 50-201 Pro / l .5; and rior to 8 stack is stack is	U2 wit 703403 th ESXid 15.5 wi 703403 Player 3 Fusion 8.5.6 ha memor may all de on tl	hout 3-SG, 600- thout 1-SG; 12.x Pro / eve an	mwa ecur ories 2017	://www are.com/ ity/advi s/VMSA- 7- 6.html	s	A-OS- VMW- ESXI/- 210617/ 223
		0	perat								
Broadcom											
Bcm43xx Wi-fi	Chipset Firmw	are									
Execute Code	04-06-2017	7.5	allow arbitr vector	remote ary cod	e attacl le via u the "Br	ınspeci oadpw	execute	w.l. om 17 .ht pw rei con ng an	cps://wv blackhat n/us- /briefing ml#broa vn- notely- mpromis -android d-ios-via bug-in-	gs ad	0-BR0- BCM43- 210617/ 224
CV Scoring Scale (CVS	S)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9 9-10
Vulnerability Type(s)											

			broadcoms- wi-fi- chipsets							
Buffalotech Wnc01wh Fir	mwara									
DoS	09-06-2017	4.3	Buffalo WNC01WH devices with firmware version 1.0.0.8 and earlier allow remote attackers to cause a denial of service against the management screen via unspecified vectors. CVE ID: CVE-2016-7821 http://buffa lo.jp/suppor t_s/s201612 01.html 225							
Bypass	09-06-2017	6.5	Buffalo NC01WH devices with firmware version 1.0.0.8 and earlier allows authenticated attackers to bypass access restriction to enable the debug option via unspecified vectors. CVE ID: CVE-2016-7824 http://buffa lo.jp/suppor t_s/s201612 210617 226 D1.html 226							
CSRF	09-06-2017	6.8	Cross-site request forgery (CSRF) vulnerability in Buffalo WNC01WH devices with firmware version 1.0.0.8 and earlier allows remote attackers to hijack the authentication of a logged in user to perform unintended operations via unspecified vectors. CVE ID: CVE-2016-7822 http://buffa lo.jp/suppor t_s/s201612 210617 227 01.html							
Ceragon										
Fiberair Ip-10) Firmware									
NA	01-06-2017	7.5	Ceragon FibeAir IP-10 have a default SSH public key in the authorized_keys file for the mateidu user, which allows remote attackers to obtain SSH access by leveraging knowledge of the Gain Privileges key. CVE ID: CVE-2015-0936							
Compulab										
	mware; Mintbox									
NA	06-06-2017	7.2	CompuLab Intense PC and MintBox NA O-COM- 2 devices with BIOS before 2017- 05-21 do not use the CloseMnf 210617							
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-							
Vulnerability Type(s): DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable										

CV Scoring Scale (CVS		0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Fortios Execute Code XSS	01-06-2017	4.3	A Cross-Site Scripting vulnerability in Fortinet FortiGate 5.2.0 through 5.2.10 allows attacker to execute unauthorized code or commands via the srcintf parameter during Firewall Policy Creation. CVE ID: CVE-2017-3127 https://forti guard.com/ psirt/FG-IR- 210617/ 233
Fortinet			
CSRF	09-06-2017	6.8	Corega CG-WLR300NX firmware Ver. 1.20 and earlier allows an attacker on the same network segment to bypass access restriction to perform arbitrary operations via unspecified vectors. CVE ID: CVE-2016-7811 Cross-site request forgery (CSRF) vulnerability in Corega CG-WLR300NX firmware Ver. 1.20 and earlier allows remote attackers to hijack the authentication of logged in user to conduct unintended operations via unspecified vectors. CVE ID: CVE-2016-7809 http://coreg a.jp/support /300nx.htm http://coreg a.jp/support /210617/ 231 CG-WL-V-V-V-V-V-V-V-V-V-V-V-V-V-V-V-V-V-V-
Cg-wlr300nx Fi	irmware		CVE ID: CVE-2016-7808
Cg-wlbaragm F XSS	09-06-2017	4.3	Cross-site scripting vulnerability in Corega CG-WLBARGMH and CG-WLBARGNL allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. http://coreg a.jp/support /security/2 210617/ 23
Corega Ca wilhangam I	Einmurano, Ca u	lhananl	Firmonara
			protection of flash memory regions, which allows local users to install a firmware rootkit by leveraging administrative Gain Privilegesileges. CVE ID: CVE-2017-8083
			protection mechanism for write 229

Google											
Android											
NA	06-06-2017	4.3	addr oper Addr allov victin page	ess bar ating sy ess Bar vs remo m by di	in all Aystems Spoot Ste atta splayin	g a mal domai	from ich o trick a	NA	1		0-G00- ANDRO- 210617/ 234
Gain Information	06-06-2017	4.3	relea kern Thro vuln exist	In TrustZone in all Android releases from CAF using the Linux kernel, an Information Exposure Through Timing Discrepancy vulnerability could potentially exist. CVE ID: CVE-2014-9951						d.c ity	O-GOO- ANDRO- 210617/ 235
Gain Information	06-06-2017	4.3	relea kern vuln exist	In TrustZone in all Android releases from CAF using the Linux kernel, an Information Exposure vulnerability could potentially exist. CVE ID: CVE-2014-9947					cps://so androio n/secur ulletin/ -05-01	d.c ity	O-GOO- ANDRO- 210617/ 236
NA	13-06-2017	4.3	using cond pote mem	g the Li lition ex	nux kei kists in leading ite.	to an a		ce. on /b	cps://sc androic n/secur ulletin/ -06-01	d.c ity	0-G00- ANDR0- 210617/ 237
Gain Information	13-06-2017	4.3	using conti initia pote kern	In all Android releases from CAF using the Linux kernel, userspace-controlled parameters for flash initialization are not sanitized potentially leading to exposure of kernel memory. CVE ID: CVE-2017-8239					ps://so androio n/secur ulletin/ -06-01	d.c ity	O-GOO- ANDRO- 210617/ 238
NA	13-06-2017	4.3	using struc prop	In all Android releases from CAF using the Linux kernel, a memory structure in a camera driver is not properly protected. CVE ID: CVE-2017-8235					ps://so androio n/secur ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 239
NA	13-06-2017	4.3	usin	g the Li	nux kei	ases fro nel, a k all of it	GSL ioc	tl ce.	ps://sc androic 1/secur	d.c	0-G00- ANDRO- 210617/
CV Scoring Scale (CVSS	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	9 9-10	

			_	meters ID: CV I	E-2017	-7366			ulletin/ -06-01	20	240
NA	13-06-2017	4.3	using valid was	using the Linux kernel, some validation of secure applications						d.c ity	O-GOO- ANDRO- 210617/ 241
NA	13-06-2017	4.3	using region	using the Linux kernel, some regions of memory were not						d.c ity	O-GOO- ANDRO- 210617/ 242
NA	13-06-2017	4.3	usin; was	In all Android releases from CAF using the Linux kernel, libtomcrypt was updated. CVE ID: CVE-2016-10335					cps://sc androic n/secur ulletin/ -06-01	d.c ity	O-GOO- ANDRO- 210617/ 243
NA	13-06-2017	4.3	using dyna coul	In all Android releases from CAF using the Linux kernel, a dynamically-protected DDR region could potentially get overwritten. CVE ID: CVE-2016-10334					cps://so androio 1/secur ulletin/ -06-01	d.c ity	O-GOO- ANDRO- 210617/ 244
NA	13-06-2017	4.3	using syste calle	g the Li em call d by HI	was all	nel, a s owed to	ensitive be	ce.	cps://sc android n/secur ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 245
NA	13-06-2017	4.3	using prot secu	g the Li ection v re appl	oid relea nux kei was not ications E-2016	nel, sta enable s.	ick d for	ce. on /b	ps://sc androic n/secur ulletin/ -06-01	d.c ity	O-GOO- ANDRO- 210617/ 246
Gain Information	13-06-2017	4.3	usin was	In all Android releases from CAF using the Linux kernel, a DRM key was exposed to QTEE applications. CVE ID: CVE-2015-9032				ce. s. on /b	cps://sc androic n/secur ulletin/ -06-01	d.c ity	O-GOO- ANDRO- 210617/ 247
Gain Information	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, a TZ memory address is exposed to HLOS by HDCP. CVE ID: CVE-2015-9031						ps://sc androic n/secur ulletin/ -06-01	d.c ity	O-GOO- ANDRO- 210617/ 248
NA	13-06-2017	4.3	In all Android releases from CAF using the Linux kernel, some						ps://so androio		O-GOO- ANDRO-
CV Scoring Scale (CVS	SS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	9-10

CV Scoring Scale (CVSS))	0-1	1-2	2-3	3-4	4-5	5-6	(6-7	7-8	8-	-9	9-10
Bypass Gain	14-06-2017	4.3	Infor	mation	disclo	sure			http	os://so	ur	0-G0	00-
Bypass Gain Information	14-06-2017	4.3	Andr CVE An e vulne enable apple of its is rate local requ Vers Andr CVE	5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-33899337. CVE ID: CVE-2017-0646 An elevation of Gain Privileges vulnerability in Bluetooth could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it is a local bypass of user interaction requirements. Product: Android. Versions: 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-35385327.				е	ce.a om, /bu 17-	os://so android /securi illetin/ 06-01	l.c ity 20	0-G0 AND 2106 253	RO- 17/
info	14-06-2017	4.3	vulna comp malia data level Mod the val	vulnerability in Bluetooth component could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate due to details specific to the vulnerability. Product: Android. Versions: 4.4.4, 5.0.2,						os://so android /securi llletin/ 06-01	d.c ity	O-GO AND 2106 252	RO-
info	14-06-2017	4.3	An ir vulne enable apple of its is rate data Andre 6.0.1	enabled. CVE ID: CVE-2015-9021 An information disclosure vulnerability in libziparchive 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: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36392138. CVE ID: CVE-2017-0647 An information disclosure /bulletin/20 ce.android.c om/security /bulletin/20 17-06-01 17-06-01 https://sour				20 our d.c ity	2106 250 0-G0 AND 2106 251	00- RO-			
NA	13-06-2017	4.3	expo CVE In all using	sed to (ID: CVI Andro g the Li	QTEE a E -2015 id relea nux kei	-9024 ises fro nel, acc	m CAF	•	/bu 17- http ce.a	/securi illetin/ 06-01 os://so indroid /securi	20 our	2106 249 0-G0 AND	00- RO-

CV Scoring Scale (CVSS	(i)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
DACCUCC GOUC	11 00 2017	6.8	vulnerability in System UI component could enable an attacker using a specially crafted						tps://so androic n/secur ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 258
Execute Code	14-06-2017	process. This issue is rated as H due to the possibility of remote code execution in an application that uses this library. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37104170. CVE ID: CVE-2017-0663					of an unGain Privilegesileged 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: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37104170.				
Execute Code	14-06-2017	6.8	vuln enab spec	mote co erabilit ole an at ially cra crary co	y in lib: ttacker afted fil	kml2 co using a e to exe		ce. on /b	tps://so androic n/securi ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 257
Gain Information	13-06-2017	5.8	using over cont	l Andro g the Li wite se ents of ID: CVI	nux ker cure me the key	nel, HL emory o store.	OS can or read	ce. on /b	tps://so androic n/securi ulletin/ -06-01	d.c	0-G00- ANDRO- 210617/ 256
DoS	08-06-2017	5	in Ar trigg poin crasl	ndroid a ger a de ter der	allows a nial of s eferenc	nttacker service e and p	(null	ub pa	tps://gi .com/al rk07/B nark/iss /1	ex z	0-G00- ANDRO- 210617/ 255
Information			comy mali data level beca oper isola appl Vers 6.0.1 A-35	ponent cious apoutside s. This use it is ating sy te applications: 4.	could epplication of its plants is a general section section 4.4, 5.0 1.1, 7.1	on to accept the control of the cont	ccess sion as High ass for ons that om othe lroid.	on /b 17	androic n/secur ulletin/ -06-01	ity	ANDRO- 210617/ 254

			is rat remo an un proc Vers A-36	ted as I ote arbi nGain F ess. Pro ions: 7. 36830	High beotrary corrivilego Orivilego Oduct: A 1.1, 7.1	ocess. T cause it ode exe esileged android .2. And	is a cution i l	in			
DoS	14-06-2017	7.1	A rer vulne enab spec device rated poss service Vers 6.0.1	mote de erabilit le an afially crace hang las Higibility (fice. Profions: 4.	y in Me ttacker afted fil or reb sh seven of remo duct: A 4.4, 5.0	service diaserve to use a e to cau oot. This due te deniandroid. 12, 5.1.1	rer coulance is ear coulance a sissue to the alof	d ce. on /b	tps://sc androic n/secur ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 259
DoS	14-06-2017	7.1	vulne enab spec device rated poss service Vers 7.1.1	vulnerability in Mediaserver could enable an attacker to use a						d.c ity	0-G00- ANDRO- 210617/ 260
DoS	14-06-2017	7.1	A rer vulne Medi attac file to rebo seve remo Andr 6.0.1 A-34	note de erabilit iaserve eker to o cause ot. This rity due ote den roid. Ve , 7.0, 7.	enial of y in lib r could use a special devices issue is the issue is the isl of seconds: 1.1, 7.1	service hevc in enable ecially ce hang s rated possible rvice. F 5.0.2, 5	an crafted or as High lity of roduct .1.1, 6.0	ce. on /b 17	tps://so androic n/secur ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 261
DoS	14-06-2017	7.1			enial of y in lib	service vpx in			https://sour ce.android.c		O-GOO- ANDRO-
CV Scoring Scale (CVSS	g Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6				6-7	7-8	8-	9 9-10			

CV Scoring Scale (CVS	S)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8	-9	9-10		
NA	06-06-2017	9.3	in all using	Andro g the Li	Power id relea nux ker ccess C	ses fro nel, an		CE	ttps://so e.androic m/securi oulletin/	l.c ity	O-GO AND 2100 273			
NA	06-06-2017	9.3	releases from CAF using the Linux kernel, a Double Free vulnerability could potentially exist. CVE ID: CVE-2015-9007				releases from CAF using the Linux ce.and kernel, a Double Free vulnerability could potentially exist.				ttps://so e.androic m/securi oulletin/ 7-05-01	l.c ity 20	272	0RO- 617/
NA	06-06-2017	9.3	relea kern Use l could CVE	ises fro el, a Tii Race Co d poten ID: CV I	ne-of-C onditior tially e E -2016	using tl heck T vulner xist. -10297	ne Linux ime-of- rability	x ce or /t 17	ttps://so e.androic m/securi oulletin/ 7-05-01	l.c ity 20	271	0RO- 617/		
			malicarbit of the Mod complete candidates the inverse 3446 ALPS	cious aperary content of the content	pplication of the polication o	on to end on the issue is it first in ocess a bility specific the impartion of the imparties of the impartie	context rated a requires nd pecific pact of d. o: A-	/t s / 17	m/securi oulletin/ 7-06-01	•	2100 270	617/		
Execute Code	14-06-2017	7.6	Secu CVE An e	re Disp ID: CV I levation	E-2014	-9966 n Privil	egesile	ge ht	oulletin/ 7-06-01 ttps://so	ur	0-G0 AND			
NA	13-06-2017	7.6	using chec	g the Li k Time	-of-use	nel, a T (TOCT)	Cime-of- OU) Rac	e or	ttps://so e.androic m/securi	l.c ity				
NA	13-06-2017	7.6	using chec Cond	g the Li k Time litions (nel, tin (TOCT) severa		ce or	ttps://so e.androic m/securi oulletin/ 7-06-01	l.c ity	O-G(AND 2100 268			
					r of a so E -2017		river.	,	oulletin/ 7-06-01	20	267			

			exist	erabilit :. ID: CV I			tially		17-	05-01			
Overflow	06-06-2017	9.3	relea kern Buffo coul	rustZon ises fro el, an Ii er Over d poten ID: CVI	m CAF nteger (flow vu tially e	using t Overflo Ilnerab xist.	he Lin w to	ux	ce.a	ps://so android /secur ılletin/ 05-01	d.c ity	AN	GOO- IDRO- 0617/ 4
NA	06-06-2017	9.3	Andı the I vuln exist	e Secur oid rel inux ke erabilit : ID: CVI	eases fi ernel, a y could	com CA captur poten	F usin	_	ce.a om /bu	ps://so android /secur illetin/ 05-01	d.c ity	AN	GOO- IDRO- 0617/ 5
NA	06-06-2017	9.3	relea kern vuln exist	ore Kern ises fro el, an In erabilit : ID: CVI	m CAF mprope y could	using t er Auth poten	he Lin orizati		ce.a om /bu	ps://so android /secur ılletin/ ·05-01	d.c ity	AN	GOO- IDRO- 0617/ 6
NA	06-06-2017	9.3	relea kern Dere pote	rustZon ises fro el, an U iference ntially (ID: CV I	m CAF Intruste e vulne exist.	using t ed Poin rability	he Lin ter		ce.a om /bu	ps://so android /secur ılletin/ ·05-01	d.c ity	AN	GOO- IDRO- 0617/ 7
NA	06-06-2017	9.3	relea kern Arra pote	rustZon ises fro el, an Ii y Index ntially (ID: CV I	m CAF mprope vulner exist.	using t er Valid ability	he Lin lation could		ce.a om /bu	ps://so android /secur alletin/ 05-01	d.c ity	AN	GOO- IDRO- 0617/ 8
NA	06-06-2017	9.3	relea kern vuln exist	ore Kern ises fro el, a Us erabilit : : ID: CVI	m CAF e After y could	using t Free poten	he Lin tially	ux	ce.a	ps://so android /secur alletin/ 05-01	d.c ity	AN	GOO- IDRO- 0617/ 9
NA	06-06-2017	9.3	In Tr relea kern	rustZon ises fro el, an Ii erabilit	e in all m CAF mprope	Andro using t er Auth	id he Lin orizati		ce.a om /bu	ps://so androio /secur ılletin/ ·05-01	d.c ity	AN	GOO- IDRO- 0617/ 0
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6		6-7	7-8	8	3-9	9-10

			CVE	ID: CVI	E-2014	-9945					
Overflow	06-06-2017	9.3	Andr the L Over vulno exist	inux ke flow to erabilit	eases fi ernel, a Buffer y could	rom CA n Integ Overfl l poten	F using er ow	ce. on /b	ps://sou android.c n/security ulletin/20 -05-01	A 2	-G00- NDR0- 10617/ 81
NA	06-06-2017	9.3	relea kern vulno exist	el, a Nu erabilit	m CAF ıll Poin y could	using t ter Der l poten	he Linux eference	ce.	ps://sou android.c n/security ulletin/20 -05-01	A 2	-G00- NDR0- 10617/ 82
NA	06-06-2017	9.3	from Use o vulno exist	of Unini erabilit	sing the itialize y could	e Linux d Varia l poten	kernel, ble	a ce.	eps://sou android.c n/security ulletin/20 -05-01	A 2 2 2 2 2	-G00- NDR0- 10617/ 83
NA	06-06-2017	9.3	from Use A pote	CAF us	sing the ee vuli exist.	e Linux nerabili	releases kernel, ity could	a ce. l on	ps://sou android.c n/security ulletin/20 -05-01	A A	-G00- NDR0- 10617/ 84
Overflow	06-06-2017	9.3	from Use o vulno exist	CAF us of Out-c erabilit	sing the of-rang y could	e Linux e Point l poten	releases kernel, er Offse tially	a ce. t on /b	ps://sou android.c n/security ulletin/20 -05-01	A 2	-G00- NDR0- 10617/ 85
Overflow	06-06-2017	9.3	from Buffe of In pote	CAF us	sing the withounerabil exist.	e Linux ut Chec ity cou	eleases kernel, king Siz ld	a ce. e on /b	ps://sou android.c n/security ulletin/20 -05-01	A 2	-G00- NDR0- 10617/ 86
Overflow	06-06-2017	9.3	CAF Buffe of In pote	using tl	he Linu withou nerabil exist.	x kerno ut Chec ity cou	king Siz	ce. e on /b	ps://sou android.c n/security ulletin/20 -05-01	A 2	-G00- NDR0- 10617/ 87
NA	06-06-2017	9.3		NSS in a	•		_		ps://sou		-G00-
CV Scoring Scale (CVS		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Use A	After Fr	ee vulr	ierabili	kernel, ty could	l on	androic 1/secur ulletin/ -05-01	ity	ANDRO- 210617/ 288
Overflow	06-06-2017	9.3	In Hill from Buffe of In pote	DR in a CAF user Copy put vul	ll Andro sing the withou nerabil	oid rele Linux at Checl ity coul	kernel, king Siz	htta ce. e on	tps://sc androic n/secur ulletin/ -05-01	d.c ity	0-G00- ANDRO- 210617/ 289
NA	06-06-2017	9.3	CAF Sign Erro	using t ed to U r could	Android he Linu nsigned potent E-2014	x kerne l Conve ially oc	rsion	ce. on /b	tps://so androio 1/secur ulletin/ -05-01	d.c ity	0-G00- ANDRO- 210617/ 290
Overflow	06-06-2017	9.3	CAF Buffe of In pote	using ther Copy put vulutially	he Linu withou nerabil	x kerne it Checl ity coul	king Siz	ce. e on /b	tps://sc androic n/secur ulletin/ -05-01	d.c ity	0-G00- ANDRO- 210617/ 291
Overflow	13-06-2017	9.3	using over WLA mess	g the Li flow vu .N func sage ler		nel, a b llity exi e to an	uffer	ce. on ct /b	tps://so androic n/secur ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 292
Overflow	13-06-2017	9.3	In all using drive over	l Andro g the Li er has a -read v	oid relea nux ken in off-by ulneral E-2017	nses fro nel, a k y-one b oility.	ernel	ce. on /b	tps://so androic n/secur ulletin/ -06-01	d.c ity	O-GOO- ANDRO- 210617/ 293
Overflow	13-06-2017	9.3	using over came	g the Li flow vu era fund	id relea nux kei ilnerabi ction. E-2017	nel, a b lity exi	uffer	ce. on /b	tps://so androio 1/secur ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 294
Overflow	13-06-2017	9.3	In all using over load	l Andro g the Li flow vu ing a fir	id relea nux kei	nses fro nel, a b llity exi image.	uffer sts whil	htt ce. e on /b	tps://so androic n/secur ulletin/ -06-01	d.c ity	O-GOO- ANDRO- 210617/ 295
Overflow	13-06-2017	9.3			id relea nux kei				tps://sc androic		O-GOO- ANDRO-
CV Scoring Scale (C	EVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (C	CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Overflow	13-06-2017	9.3			id relea nux kei				ps://so androio		O-GOO- ANDRO-
Overflow	13-06-2017	9.3	using over strin CVE	g the Li read ca g is not ID: CV I	NULL E-2017	rnel, a b r if a pa termina -7365	ouffer rticular ated.	ce. om /bi	ps://so androio /secur ulletin/ -06-01	l.c ity 20	O-GOO- ANDRO- 210617/ 303
NA	13-06-2017	9.3	using unde whil CVE	g the Li erflow v e proce ID: CV I	vulnera ssing tl E -2017	nel, an bility e ne boot -7367	integer xists image.	ce. om /bi	ps://so androio n/secur ulletin/ -06-01	d.c ity 20	0-G00- ANDRO- 210617/ 302
NA	13-06-2017	9.3	using inde prop leadi CVE	g the Li x in an erly va ing to k ID: CV I	E-2017	rnel, an outine i g poten tack cor -7369	array s not tially rruptior	ce. om /bi	ps://sc androic n/secur ulletin/ -06-01	d.c ity 20	0-G00- ANDRO- 210617/ 301
NA	13-06-2017	9.3	using poin has b turn	g the Li ter is po been fre ed off b	id releanux kenotentia otentia eed who y Bluet E-2017	nel, a d lly used en SLIM ooth.	lata I after it	ce.	ps://so androio 1/secur ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 300
NA	13-06-2017	9.3	using free displ	g the Li vulnera lay driv ID: CV I	E-2017	rnel, a d xists in -7373	louble a	ce. om /bi	ps://so androio /secur ulletin/ -06-01	d.c ity 20	0-G00- ANDRO- 210617/ 299
NA	13-06-2017	9.3	Ando the I miss pote bour	roid relainux ke ing whe ntially lads hea	eases fi ernel, a	om CA bounds ing into to an o	n in all F using s check o an arra ut-of-	ce. is om	ps://sc androic n/secur ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 298
NA	13-06-2017	9.3	In all using bour occu	l Andro g the Li nds acce r in a ca	E-2017 id relea nux ken ess can amera f E-2017	nses fro nel, an potenti unction	out of ally	htt ce. om /bi	-06-01 ps://sc androic l/secur ulletin/ -06-01	d.c ity	0-G00- ANDRO- 210617/ 297
			IPA (driver.		-	sts in ar	/bi	n/secur ulletin/	-	210617/ 296

CV Scoring Scale (C	CVSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-10
IVA	13-00-2017		using the Linux kernel, an untrusted pointer dereference vulnerability exists in WideVine	ce.android.c om/security /bulletin/20	ANDRO- 210617/ 312
NA	13-06-2017	9.3	using the Linux kernel, a buffer overflow vulnerability exists in a cryptographic routine. CVE ID: CVE-2015-9028 In all Android releases from CAF	ce.android.c om/security /bulletin/20 17-06-01 https://sour	ANDRO- 210617/ 311
NA Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a vulnerability exists in the access control settings of modem memory. CVE ID: CVE-2015-9029 In all Android releases from CAF	https://sour ce.android.c om/security /bulletin/20 17-06-01 https://sour	0-G00- ANDR0- 210617/ 310
Bypass	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, the Hypervisor API could be misused to bypass authentication. CVE ID: CVE-2015-9030	https://sour ce.android.c om/security /bulletin/20 17-06-01	O-GOO- ANDRO- 210617/ 309
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a QTEE system call fails to validate a pointer. CVE ID: CVE-2015-9033	https://sour ce.android.c om/security /bulletin/20 17-06-01	O-GOO- ANDRO- 210617/ 308
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, there was an issue related to RPMB processing. CVE ID: CVE-2016-10338	https://sour ce.android.c om/security /bulletin/20 17-06-01	O-GOO- ANDRO- 210617/ 307
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, an integer underflow leading to buffer overflow vulnerability exists in a syscall handler. CVE ID: CVE-2016-10340	https://sour ce.android.c om/security /bulletin/20 17-06-01	0-G00- ANDR0- 210617/ 306
NA	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, 3rd party TEEs have more Gain Privilegesilege than intended. CVE ID: CVE-2016-10341	https://sour ce.android.c om/security /bulletin/20 17-06-01	0-G00- ANDR0- 210617/ 305
			overflow vulnerability exists in a syscall handler. CVE ID: CVE-2016-10342	om/security /bulletin/20 17-06-01	210617/ 304

			DRM		E 2015	0027		17	'-06-01			
NA	13-06-2017	9.3	In all using untr vuln DRM	ID: CVI Andro g the Li usted p erabilit	id relea nux kei ointer (y exists	ises fro nel, an derefer in Wic	ence	ce on /b	tps://sc .androic n/secur ulletin/ '-06-01	l.c ity	0-G0 ANDI 2106 313	RO-
Overflow	13-06-2017	9.3	In all using over QTE	l Andro g the Li	id relea nux kei lnerabi cation.	nses fro nel, a b llity exi		ce on /b	tps://so .androio n/secur oulletin/ '-06-01	l.c ity	0-G0 ANDI 2106 314	RO-
Overflow	13-06-2017	9.3	using over Play	Androg the Liflow vu Ready A	nux kei Inerabi API.	nel, a b lity exi		ce ne on /b	tps://so .androio n/secur oulletin/ '-06-01	l.c ity	0-G0 ANDI 2106 315	RO-
NA	13-06-2017	9.3	using untr vuln unlo	l Andro g the Li usted p erabilit cking o ID: CV I	nux kei ointer (y exists f memo	nel, an derefer in the ory.		ce on /b	tps://sc .androic n/secur oulletin/ '-06-01	l.c ity	0-G0 ANDI 2106 316	RO-
NA	13-06-2017	9.3	using untr vuln DRM	Androg the Liusted perabilit	nux kei ointer (y exists	nel, an derefer s in Wic	ence	ce on /b	tps://sc .androic n/secur ulletin/ '-06-01	l.c ity	0-G0 ANDI 2106 317	RO-
NA	13-06-2017	9.3	using vuln of an	l Andro g the Li erabilit SCM ca ID: CVI	nux kei y exists all.	nel, a in the	m CAF parsing	ce on /b	tps://so .androio n/secur oulletin/ '-06-01	d.c ity	0-G0 ANDI 2106 318	RO-
Overflow	13-06-2017	9.3	using over debu	Androg the Liflow vulg funct ID: CV	nux kei lnerabi ionality	nel, an llity exi 7.	integer	ce on /b	tps://so .androio n/secur oulletin/ '-06-01	d.c ity	0-G0 ANDI 2106 319	RO-
Overflow	13-06-2017	9.3	In all Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in WideVine DRM. https://sour ce.android.c om/security /bulletin/20				d.c ity	O-GO ANDI 2106 320	RO-			
CV Scoring Scale (C	VSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	.9	9-10

				7-06-01
NA	13-06-2017	9.3	using the Linux kernel, a vulnerability exists in the parsing of a DRM provisioning command. CVE ID: CVE-2014-9962 CVE ID: CVE-2014-9962	ttps://sour O-G00- e.android.c ANDRO- m/security 210617/ bulletin/20 321 7-06-01
Bypass	13-06-2017	9.3	using the Linux kernel, a vulnerability in eMMC write protection exists that can be used //	ttps://sour e.android.c m/security bulletin/20 7-06-01
Overflow	13-06-2017	9.3	using the Linux kernel, a buffer overflow vulnerability exists in the PlayReady API.	ttps://sour 0-G00- e.android.c ANDRO- m/security 210617/ bulletin/20 323 7-06-01
Execute Code Overflow Memory Corruption	14-06-2017	9.3	vulnerability in libhevc in Mediaserver could enable an attacker using a specially crafted /I	ttps://sour e.android.c m/security bulletin/20 7-06-01
Huawei				
Ar1220 Firmwa		4.0	II: AD4222	11 - 11 O 1111
DoS	08-06-2017	4.3	software before V200R005SPH006 allow remote attackers to cause a denial of service (board reset) via vectors involving a large amount of traffic from the GE port to the FE port.	ttp://www O-HUA- nuawei.com AR122- en/securit /psirt/secu 325 tty- ulletins/se urity- dvisories/h

				417840.htm					
Oceanstor Uds	Firmware								
Gain Information	08-06-2017	5	The DeviceManager in Huawei OceanStor UDS devices with software before V100R002C01SPC102 might allow remote attackers to obtain sensitive information via a crafted UDS patch with JavaScript. CVE ID: CVE-2015-2251	http://www 1.huawei.co m/en/secur ity/psirt/se curity- bulletins/se curity- advisories/h w- 417837.htm	O-HUA- OCEAN- 210617/ 326				
Execute Code	08-06-2017	9.3	Huawei OceanStor UDS devices with software before V100R002C01SPC102 might allow remote attackers to execute arbitrary code with root Gain Privilegesileges via a crafted UDS patch with shell scripts. CVE ID: CVE-2015-2252	http://www 1.huawei.co m/en/secur ity/psirt/se curity- bulletins/se curity- advisories/h w- 417837.htm	O-HUA- OCEAN- 210617/ 327				
Firmware; S97		iware; S	6300 Firmware; S6700 Firmware;	57700 Firmw	are; 5 9300				
DoS	08-06-2017	7.8	The user authentication module in Huawei Campus switches S5700, S5300, S6300, and S6700 with software before V200R001SPH012 and S7700, S9300, and S9700 with software before V200R001SPH015 allows remote attackers to cause a denial of service (device restart) via vectors involving authentication, which trigger an array access violation. CVE ID: CVE-2015-2800	http://www .huawei.com /en/securit y/psirt/secu rity- bulletins/se curity- advisories/h w- 418554.htm	O-HUA- S5300- 210617/ 328				
Iodata Ts-wrla Firmw	aro:Tc-wrln Fir	mwaro							
Gain	09-06-2017	5	I-O DATA DEVICE TS-WRLP	http://xananar	O-IOD-				
Information	09-00-2017	3	firmware version 1.00.01 and earlier and TS-WRLA firmware version 1.00.01 and earlier allow remote attackers to obtain	http://www .iodata.jp/su pport/infor mation/201 6/ts-wrlap/	TS-WR- 210617/ 329				
CV Cooping Co-1- (CVC)		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8 8	9-10				
CV Scoring Scale (CVSS)									
Vulnerability Type(s): DoS- Denial of Service		iest Forgery	; XSS- Cross Site Scripting; Sql- SQL Injection; NA: No	t Applicable					

			authentication credentials via unspecified vectors. CVE ID: CVE-2016-7814		
Execute Code Overflow	09-06-2017	9	Buffer overflow in I-O DATA DEVICE TS-WRLP firmware version 1.01.02 and earlier and TS-WRLA firmware version 1.01.02 and earlier allows an attacker with administrator rights to cause a denial-of-service (DoS) or execute arbitrary code via unspecified vectors. CVE ID: CVE-2016-7820	http://www .iodata.jp/su pport/infor mation/201 6/ts- wrlap_2/	0-I0D- TS-WR- 210617/ 330
Execute Code	09-06-2017	9	I-O DATA DEVICE TS-WRLP firmware version 1.01.02 and earlier and TS-WRLA firmware version 1.01.02 and earlier allows an attacker with administrator rights to execute arbitrary OS commands via unspecified vectors. CVE ID: CVE-2016-7819	http://www .iodata.jp/su pport/infor mation/201 6/ts- wrlap_2/	0-IOD- TS-WR- 210617/ 331
Wfs-sr01 Firm	ware				
Bypass	09-06-2017	5	I-O DATA DEVICE WFS-SR01 firmware version 1.10 and earlier allow remote attackers to bypass access restriction to access data on storage devices inserted into the product via unspecified vectors. CVE ID: CVE-2016-7807	http://www .iodata.jp/su pport/infor mation/201 6/wfs-sr01/	0-I0D- WFS-S- 210617/ 332
Execute Code	09-06-2017	10	I-O DATA DEVICE WFS-SR01 firmware version 1.10 and earlier allow remote attackers to execute arbitrary OS commands via unspecified vectors. CVE ID: CVE-2016-7806	http://www .iodata.jp/su pport/infor mation/201 6/wfs-sr01/	0-I0D- WFS-S- 210617/ 333
Linux					
Linux Kernel					
Execute Code	14-06-2017	9.3	An elevation of Gain Privilegesilege vulnerability in the kernel FIQ debugger could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as	https://sour ce.android.c om/security /bulletin/20 17-06-01	O-LIN- LINUX- 210617/ 334
CV Scoring Scale (CVS		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8 8	9-10

			High 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-36101220. CVE ID: CVE-2017-0648		
Paloaltonetwo	rks				
Pan-os					
Execute Code	01-06-2017	9.3	Palo Alto Networks Panorama VM Appliance with PAN-OS before 6.0.1 might allow remote attackers to execute arbitrary Python code via a crafted firmware image file. CVE ID: CVE-2015-6531	NA	O-PAL- PAN-O- 210617/ 335
Peplink					
	ware; 2500 Fi	rmware	; 380hw6 Firmware; 580hw2 Firmv	ware; 710hw3	Firmware;
B305hw2 Firm	1				
XSS	05-06-2017	4.3	XSS via orig_url exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_380hw6_580hw2_710h w3_1350hw2_2500-7.0.1-build2093. The affected script is guest/preview.cgi. CVE ID: CVE-2017-8839	NA	O-PEP- 1350H- 210617/ 336
XSS	05-06-2017	4.3	XSS via syncid exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw- b305hw2_380hw6_580hw2_710h w3_1350hw2_2500-7.0.1- build2093. The affected script is cgi-bin/HASync/hasync.cgi. CVE ID: CVE-2017-8838	NA	O-PEP- 1350H- 210617/ 337
Gain Information	05-06-2017	5	Debug information disclosure exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_380hw6_580hw2_710h w3_1350hw2_2500-7.0.1-	NA	O-PEP- 1350H- 210617/ 338

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s):										

NA	05-06-2017	5	bin/F show Numl and S CVE I	HASync s Maste per, HA lubmitt D: CVE	direct /hasyn er LAN Group ed synd -2017 ssword	I	Λ		O-PEP-		
			on Per 710, firmv b305 w3_1 build /etc/ case of comp access them syste CVE I	eplink E 1350, a vare be hw2_38 350hw 2093. T waipas one of t oromise s to pas to com ms.	Falance and 250 fore fw 30hw6. 2.2500 he files and / hese de do the assword promis	alance 305, 380, 580, and 2500 devices with Fore fw- Ohw6_580hw2_710h 2_2500-7.0.1- the files in question are and /etc/roapass. In these devices is d, the attacker can gain swords and abuse promise further -2017-8837					1350H- 210617/ 339
Execute Code; CSRF	05-06-2017	6.8	305, 3 device b305 w3_1 build admi affect exect user can for the creating	CSRF exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_380hw6_580hw2_710h w3_1350hw2_2500-7.0.1-build2093. The CGI scripts in the administrative interface are affected. This allows an attacker to execute commands, if a logged in user visits a malicious website. This can for example be used to change the credentials of the administrative webinterface. CVE ID: CVE-2017-8836							O-PEP- 1350H- 210617/ 340
Directory Traversal	05-06-2017	7.5	Pepli 1350 firmv b305 w3_1 build is abs	nk Bala , and 2! vare be hw2_3! 350hw 2093. T solute p	nce 30 500 dev fore fw 30hw6_ 2_2500 'he atta ath tra /firmw	580hw	ву	A	O-PEP- 1350H- 210617/ 341		
CV Scoring Scale (CVSS))	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-	9 9-10

			CVE ID: CVE-2017-8841		
Sql	05-06-2017	7.5	SQL injection exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw- b305hw2_380hw6_580hw2_710h w3_1350hw2_2500-7.0.1- build2093. An attack vector is the bauth cookie to cgi- bin/MANGA/admin.cgi. One impact is enumeration of user accounts by observing whether a session ID can be retrieved from the sessions database. CVE ID: CVE-2017-8835	NA	O-PEP- 1350H- 210617/ 342
Phoenixbroad	band		0.2.2.0.2.202.		
Poweragent Sc	:3 Bms Firmwa	re			
NA	02-06-2017	5	A Use of Hard-Coded Password issue was discovered in Phoenix Broadband PowerAgent SC3 BMS, all versions prior to v6.87. Use of a hard-coded password may allow unauthorized access to the device. CVE ID: CVE-2017-6039	NA	0-PHO- POWER- 210617/ 343
Redhat					
Enterprise Line Workstation	ux Desktop; Ent	erprise	Linux Hpc Node; Enterprise Linux Se	rver; Enterpr	ise Linux
info	08-06-2017	5	389 Directory Server in Red Hat Enterprise Linux Desktop 6 through 7, Red Hat Enterprise Linux HPC Node 6 through 7, Red Hat Enterprise Linux Server 6 through 7, and Red Hat Enterprise Linux Workstation 6 through 7 allows remote attackers to read the default Access Control Instructions. CVE ID: CVE-2016-5416	https://bug zilla.redhat. com/show_ bug.cgi?id=1 349540	O-RED- ENTER- 210617/ 344
NA	08-06-2017	5	389 Directory Server in Red Hat Enterprise Linux Desktop 6 through 7, Red Hat Enterprise Linux HPC Node 6 through 7, Red Hat Enterprise Linux Server 6 through 7, and Red Hat Enterprise	https://bug zilla.redhat. com/show_ bug.cgi?id=1 358865	O-RED- ENTER- 210617/ 345
CV Scoring Scale (CVS	SS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			Linux Workstation 6 through 7 allows remote attackers to obtain user passwords. CVE ID: CVE-2016-5405		
Gain Information	08-06-2017	5	389 Directory Server in Red Hat Enterprise Linux Desktop 6 through 7, Red Hat Enterprise Linux HPC Node 6 through 7, Red Hat Enterprise Linux Server 6 through 7, and Red Hat Enterprise Linux Workstation 6 through 7 allows remote attackers to infer the existence of RDN component objects. CVE ID: CVE-2016-4992	https://bug zilla.redhat. com/show_ bug.cgi?id=1 347760	O-RED- ENTER- 210617/ 346
NA	08-06-2017	5	mod_ns in Red Hat Enterprise Linux Desktop 7, Red Hat Enterprise Linux HPC Node 7, Red Hat Enterprise Linux Server 7, and Red Hat Enterprise Linux Workstation 7 allows remote attackers to force the use of ciphers that were not intended to be enabled. CVE ID: CVE-2016-3099	https://bug zilla.redhat. com/show_ bug.cgi?id=1 319052	O-RED- ENTER- 210617/ 347
Execute Code	08-06-2017	7.5	SerializableProvider in RESTEasy in Red Hat Enterprise Linux Desktop 7, Red Hat Enterprise Linux HPC Node 7, Red Hat Enterprise Linux Server 7, and Red Hat Enterprise Linux Workstation 7 allows remote attackers to execute arbitrary code. CVE ID: CVE-2016-7050	https://bug zilla.redhat. com/show_ bug.cgi?id=1 378613	O-RED- ENTER- 210617/ 348
Samsung	77				
Galaxy S6 Edge Directory Traversal	07-06-2017	7.8	Directory traversal vulnerability in the WifiHs20UtilityService on the Samsung S6 Edge LRX22G.G925VVRU1AOE2 allows remote attackers to overwrite or create arbitrary files as the system-level user via a (dot dot) in the name of a file, compressed into a	NA	0-SAM- GALAX- 210617/ 349
CV Scoring Scale (CVSS	5)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	9-10
Vulnerability Type(s): DoS- Denial of Service		iest Forgery	y; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not	Applicable	

	1			Т	T
			zipped file named cred.zip, and		
			downloaded to /sdcard/Download. CVE ID: CVE-2015-7888		
Seagate			CVE ID: CVE-2015-7888		
Business Nas Fi	irmwara				
Execute Code	08-06-2017	10	Congata Puningg NAC daviged with	NA	O-SEA-
Execute Code	00-00-2017	10	Seagate Business NAS devices with firmware before 2015.00322 allow	INA	BUSIN-
			remote attackers to execute		210617/
			arbitrary code with root Gain		350
			Privilegesileges by leveraging use		
			of a static encryption key to create		
			session tokens.		
			CVE ID: CVE-2014-8687		
Sophos					
Cyberoam Firm	T			T	
XSS	07-06-2017	4.3	An XSS vulnerability allows remote	http://seclis	O-SOP-
			attackers to execute arbitrary client	ts.org/bugtr	CYBER-
			side script on vulnerable installations of Sophos Cyberoam	aq/2017/Ju n/4	210617/ 351
			firewall devices with firmware	11/ 4	331
			through 10.6.4. User interaction is		
			required to exploit this		
			vulnerability in that the target must		
			visit a malicious page or open a		
			malicious file. The specific flaw		
			exists within the handling of a		
			request to the		
			"LiveConnectionDetail.jsp" application. GET parameters		
			"applicationname" and "username"		
			are improperly sanitized allowing		
			an attacker to inject arbitrary		
			JavaScript into the page. This can		
			be abused by an attacker to		
			perform a cross-site scripting		
			attack on the user. A vulnerable		
			URI is		
			/corporate/webpages/trafficdiscov		
			ery/LiveConnectionDetail.jsp.		
			CVE ID: CVE-2016-9834		

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s):										