

National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures(CVE) Report

16 - 30 Apr 2019

Vol. 06 No. 08

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID		Par	tch	NCII	PC ID		
			Aŗ	pplica	tion					
74cms										
74cms										
Cross-Site Request Forgery (CSRF)	20-04-2019	6.8	74CMS v5.0.1 has a CSRF vulnerability to add a new admin user via the index.php?m=Admin&c=ad min&a=add URI. CVE ID: CVE-2019-11374			N/A		A-74C 74CM- 01051	-	
Apache									•	
pony_mail										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	22-04-2019	4.3	speciall enable i JavaScri interfac	red whered where y craft reflect ipt in t ce.	y was herein a ted URL ed XSS v the pony	could via v mail	N/A		A-APA PONY- 01051	-
pdfbox										
Improper Restriction of XML External Entity Reference ('XXE')	17-04-2019	7.5	Apache PDFBox 2.0.14 does not properly initialize the XML parser, which allows context-dependent attackers to conduct XML External Entity (XXE) attacks via a crafted XFDF. CVE ID: CVE-2019-0228		N/A		A-APA PDFB- 01051	-		
aquaverde										
aquarius_cms	5									
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	[Description	on & CVE	ID	Pa	tch	NCII	PC ID
Information Exposure Through Log Files	24-04-2019	5	through Informathrough an errowriter	gh 4.3.5 nation E gh Log I or in th compo	Exposure Files bec e Log-Fi	e ause of le	N/A		A-AQU- AQUA- 010519/4	
Artifex										
mujs										
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2019	7.5	Artife: Numb numto in jsnu based	x MuJS a er#toFi ostr imp imber.c buffer o	discover 1.0.5. Th xed() ar lementa have a soverflow 2019-1	nd nations stack- v.	N/A		A-ART MUJS- 01051	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2019	5	An issue was discovered in Artifex MuJS 1.0.5. jscompile.c can cause a denial of service (invalid stack-frame jump) because it lacks an ENDTRY opcode call.			N/A		A-AR7 MUJS- 01051		
Uncontrolled Resource Consumption	22-04-2019	5	CVE ID: CVE-2019-11412 An issue was discovered in Artifex MuJS 1.0.5. It has unlimited recursion because the match function in regexp.c lacks a depth check. CVE ID: CVE-2019-11413			N/A		A-ART- MUJS- 010519/		
atftp_project										
atftp										
Improper Restriction	20-04-2019 7.5 An issue was discovered in atftpd in atftp 0.7.1. A							A-ATF- ATFT-		
CV Scoring Scal (CVSS)	e 0-1 pe(s): CSRF- Cross	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
vuinerability Ty	Denial of Service	_	_	_		_			noi matio	ii, DU3-

Vulnerability Type(s)	Publish Date	cvss	De	escription	& CVE	ID	Pa	tch	NCII	PC ID
of Operations within the Bounds of a Memory Buffer			crafted stack-b due to a implem The vul trigger error p fewer. I instance strncpy code batftpd_fitftpd_m tftp_mt	•	rigger fer over arely ty is ading a 3 byte e mult s vulne within ifically file.c, ad	ing a erflow call. an s or iple erable n the within			01053	19/8
NULL Pointer Dereference	20-04-2019	4.3	atftpd i not lock thread_ before a thread result, to vulnera service pointer thread_ assigned modified before a check, to derefer	CVE ID: CVE-2019-11365 An issue was discovered in atftpd in atftp 0.7.1. It does not lock the thread_list_mutex mutex before assigning the current thread data structure. As a result, the daemon is vulnerable to a denial of		N/A		A-ATH ATFT 01052	-	
Atlassian	Atlassian									
confluence										
Improper Limitation of 18-04-2019 9 Confluence Server and Data Center had a path traversal							N/A		A-ATI CONF	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	cvss	·					tch	NCII	PC ID
a Pathname to a Restricted Directory ('Path Traversal')			down resou who hattach or blo space who hattach or blo space who hattach or blo space who hattach can le execurun a Confluctor Conflutor of the force of the forc	rability loadalla rce. A reas permanents to gs or to or a permas 'Admissions fit this parability rary located to reas to non vulneration on vulneration for 6. 12.4 on for 6. 13.5 on for 6. 14.0 because a fear	ttachments at hission to pages create a resonal spain' or a spain to write to write tions where the consistency or a spain' or	tacker o add and / new bace or ce can ersal files to hich de that ion of Data f om 2.0.0 ed om the ex), 14.3 6.14.x), re this			01051	9/10
Atutor										
atutor										
Unrestricted Upload of File with Dangerous Type	22-04-2019	6.5	An issue was discovered in ATutor through 2.2.4. It allows the user to run commands on the server with the teacher user		N/A		A-ATU ATUT- 01051			
CV Scoring Scal (CVSS) Vulnerability Ty	pe(s): CSRF- Cross	_	-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 ite Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.					9-10 n; DoS-		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			privilege. The Upload Files section in the File Manager field contains an arbitrary file upload vulnerability via upload.php. The \$IllegalExtensions value only lists lowercase (and thus .phP is a bypass), and omits .shtml and .phtml.		
DI 11			CVE ID : CVE-2019-11446		
Blackberry unified endp	oint_managen	nent			
Improper Restriction of XML External Entity Reference ('XXE')	18-04-2019	5	An XML External Entity vulnerability in the UEM Core of BlackBerry UEM version(s) earlier than 12.10.1a could allow an attacker to potentially gain read access to files on any system reachable by the UEM service account. CVE ID: CVE-2019-8999	N/A	A-BLA-UNIF- 010519/12
brassica					
soy_cms			** DISPUTED ** SOY CMS		
Improper Control of Generation of Code ('Code Injection')	20-04-2019	6.5	v3.0.2 allows remote attackers to execute arbitrary PHP code via a php substring in the second text box. NOTE: the vendor indicates that there was an assumption that the content is "made editable on its own." CVE ID: CVE-2019-11376</td <td>N/A</td> <td>A-BRA-SOY 010519/13</td>	N/A	A-BRA-SOY 010519/13

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CV33)										

burrow-wheel burrow-wheel Improper		roject			
	ler_aligner				
Improper					
Restriction of Operations	20-04-2019	7.5	BWA (aka Burrow-Wheeler Aligner) 0.7.17 r1198 has a Buffer Overflow via a long prefix that is mishandled in bns_fasta2bntseq and bns_dump at btnseq.c. CVE ID: CVE-2019-11371	N/A	A-BUR- BURR- 010519/14
Checkpoint					
zonealarm					
Untrusted Search Path	17-04-2019	2.1	Some of the DLLs loaded by Check Point ZoneAlarm up to 15.4.062 are taken from directories where all users have write permissions. This can allow a local attacker to replace a DLL file with a malicious one and cause Denial of Service to the client. CVE ID: CVE-2019-8453	N/A	A-CHE- ZONE- 010519/15
N/A	17-04-2019	4.6	A hard-link created from the log file of Check Point ZoneAlarm up to 15.4.062 to any file on the system will get its permission changed so that all users can access that linked file. Doing this on files with limited access gains the local attacker higher privileges to the file. CVE ID: CVE-2019-8455	N/A	A-CHE- ZONE- 010519/16
Cisco					

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): CSRE- Cross Site Request Forgery: Dir. Tray - Directory Trayersal: +Info- Gain Information: DoS-										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
dna_center					
Improper Input Validation	17-04-2019	5.5	A vulnerability in the Software Image Management feature of Cisco DNA Center could allow an authenticated, remote attacker to access to internal services without additional authentication. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending arbitrary HTTP requests to internal services. An exploit could allow the attacker to bypass any firewall or other protections to access unauthorized internal services. DNAC versions prior to 1.2.5 are affected. CVE ID: CVE-2019-1841	N/A	A-CIS-DNA 010519/17
expressway_s	l series				
Cross-Site Request Forgery (CSRF)	17-04-2019	4.3	A vulnerability in the FindMe feature of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to conduct a cross- site request forgery (CSRF) attack and perform arbitrary actions on an affected system. The vulnerability is due to insufficient CSRF	N/A	A-CIS-EXPR- 010519/18

 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)	Publish Date	cvss	Description & CVE ID	Pate	ch	NCIII	PC ID
			protections for the webbased management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to follow a maliciously crafted link. A successful exploit could allow the attacker to perform arbitrary actions on an affected system with the privileges of the user. The arbitrary actions include adding an attacker-controlled device and redirecting calls intended for a specific user. For more information about CSRF attacks and potential mitigations, see Understanding Cross-Site Request Forgery Threat Vectors. This vulnerability is fixed in software version X12.5.1 and later. CVE ID: CVE-2019-1722				
unified_comp	uting_system					L	
Improper Input Validation	17-04-2019	3.6	A vulnerability in the local management CLI implementation for specific commands on the Cisco UCS B-Series Blade Servers could allow an authenticated, local attacker to overwrite an arbitrary file on disk. It is also possible the attacker could inject CLI command parameters that should not	N/A		A-CIS- 01051	
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)	ac/s), CSRF, Cross	Cita Dan	uest Forgery; Dir. Trav Directory Trav	orcali Unfo	. Gain Ir	formatio	n: Dos

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
			subsect CLI convulne proper user in mana An attention and is a limit mana An exattack arbitrinject parant been ovulne softwal later.	t of local ommand rability er input input for gement cacker co- ulnerabil nticating suing a ted subsequent ploit cor eary files CLI com- neters the disabled rability are vers	is due to validation local CLI compould exposed ility by g to the crafted for cet of local cet o	ement lack of on of mands. loit device form of al mands. the an or ld have n 2a) and				
registered_en	velope_servi	ce								
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	based Regist could authe attack site so agains service due to of use web-k affect	interfactered Enticated anticated are to coeripting at anoth the Entire The volume of insufficer supplicated in the total and the entire the total and the entire the total and the entire	, remote nduct a (XSS) at er user o ulnerab cient val ied inpu terface o	Cisco Service e cross- tack of the ility is idation t by the	N/A		A-CIS- 01051	-REGI- 19/20	
CV Scoring Scale (CVSS) Vulnerability Ty	e 0-1 pe(s): CSRF- Cros Denial of Servic	_							8-9 nformatio	9-10 on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patcl	h	NCIII	PC ID
			vulnerability by sending an email with a malicious payload to another user. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. This vulnerability affects software versions 5.3.4.x. CVE ID: CVE-2019-1777				
umbrella							
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	4.3	A vulnerability in the URL block page of Cisco Umbrella could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user in a network protected by Umbrella. The vulnerability is due to insufficient validation of input parameters passed to that page. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive browserbased information. This vulnerability has been fixed in the current version of Cisco Umbrella. Cisco	N/A		A-CIS- UMBR 01051	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
	• • •	_	uest Forgery; Dir. Trav Directory Tra oss Site Scripting; Sql- SQL Injection; 10			formatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Umbrella is a cloud service.		
			CVE ID : CVE-2019-1792		
wireless_lan_	controller				
N/A	17-04-2019	6.1	A vulnerability in the handling of Inter-Access Point Protocol (IAPP) messages by Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability exist because the software improperly validates input on fields within IAPP messages. An attacker could exploit the vulnerability by sending malicious IAPP messages to an affected device. A successful exploit could allow the attacker to cause the Cisco WLC Software to reload, resulting in a DoS condition. Software versions prior to 8.2.170.0, 8.5.150.0, and 8.8.100.0 are affected.	N/A	A-CIS-WIRE- 010519/22
			CVE ID : CVE-2019-1796 A vulnerability in the web-		
Cross-Site Request Forgery (CSRF)	17-04-2019	6.8	based management interface of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to conduct a crosssite request forgery (CSRF) attack and perform arbitrary	N/A	A-CIS-WIRE- 010519/23

0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

CV Scoring Scale

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			actions on the device with the privileges of the user, including modifying the device configuration. The vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an interface user to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the device with the privileges of the user. Software versions prior to 8.3.150.0, 8.5.135.0, and 8.8.100.0 are affected. CVE ID: CVE-2019-1797		
N/A	17-04-2019	6.1	A vulnerability in the handling of Inter-Access Point Protocol (IAPP) messages by Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability exist because the software improperly validates input on fields within IAPP messages. An attacker could exploit the vulnerability by sending malicious IAPP messages to an affected device. A	N/A	A-CIS-WIRE- 010519/24

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			allow the Ci reload condi prior and 8	ssful exp the atta sco WLO d, resulti tion. Sof to 8.2.17 .8.100.0	cker to of Software volume 20.0, 8.5 are affe	cause are to DoS ersions .150.0, cted.				
N/A	17-04-2019	6.1	A vuln handl Point messa LAN (Software unaut attack service vulne the software within attack vulne malicinal an afficial succession of the Cireload condiprior and 8	nerabiliting of In Protocoages by (Controlled are could thenticate to case (DoS) rability of tware in IAPP in the attasion set of the attase o	y in the ter-Accord (IAPP) Cisco Wier (WLC) d allow ted, adjacuse a decondition of the condition of the cond	ess areless an acent nial of on. The cause erly ds s. An the ing ages to ald cause are to DoS ersions .150.0, cted.	N/A		A-CIS- 01051	-WIRE- 19/25
wireless_lan_o	controller_sof	tware								
Improper Access Control	17-04-2019	3.3	access	nerabilit s contro e Secure	l mecha	nisms	N/A		A-CIS- 01051	-WIRE- 19/26
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_				_				on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			server implementation for Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, adjacent attacker to access a CLI instance on an affected device. The vulnerability is due to a lack of proper inputand validation-checking mechanisms for inbound SSH connections on an affected device. An attacker could exploit this vulnerability by attempting to establish an SSH connection to an affected controller. An exploit could allow the attacker to access an affected device's CLI to potentially cause further attacks. This vulnerability has been fixed in version 8.5(140.0). CVE ID: CVE-2019-1805		
Improper Input Validation	17-04-2019	6.8	A vulnerability in Locally Significant Certificate (LSC) management for the Cisco Wireless LAN Controller (WLC) could allow an authenticated, remote attacker to cause the device to unexpectedly restart, which causes a denial of service (DoS) condition. The attacker would need to have valid administrator credentials. The	N/A	A-CIS-WIRE- 010519/27

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
email_securit	v annliance		vulnerability is due to incorrect input validation of the HTTP URL used to establish a connection to the LSC Certificate Authority (CA). An attacker could exploit this vulnerability by authenticating to the targeted device and configuring a LSC certificate. An exploit could allow the attacker to cause a DoS condition due to an unexpected restart of the device. CVE ID: CVE-2019-1830		
Improper Input Validation	17-04-2019	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 content filters on the device. The vulnerability is due to improper input validation of the email body. An attacker could exploit this vulnerability by inserting specific character strings in the message. A successful exploit could allow the attacker to bypass configured content filters that would normally drop the email.	N/A	A-CIS-EMAI- 010519/28

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
			CVE I	D : CVE-	2019-1	831				
unified_comm	nunications_1	nanage	r							
Improper Input Validation	17-04-2019	7.8	Data S Cisco Comm (Unificunauti attack service the m vulne impro- param reque explo sendi- the Uni device could make quit u preve the Uni GUI. M may b norm version 12.5 a	derability chenticate (DoS) anagem rability oper valineters in this vung a craft this vung a craft the A Cinexpect anting acounting acou	ons Man could all ced, rem use a de condition ent GUI. is due to dation of the UD attacker alnerabil fed requ f an affe essful en essful en essful en e attack sco DB s edly, min accommended red to red tion. Soft 11.5, 12 ted.	ager low an ote enial of on on The of input S API could lity by uest to ected exploit eer to service eess to gement tion estore ftware 2.0,	N/A		A-CIS- 01051	UNIF- 9/29
prime_netwo	rk_registrar									
Improper Initialization	17-04-2019	7.8	A vulnerability in the DHCPv6 input packet processor of Cisco Prime Network Registrar could allow an unauthenticated, remote attacker to restart				N/A		A-CIS- 01051	PRIM- 9/30
CV Scoring Scal (CVSS)	e 0-1 pe(s): CSRF- Cros	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
vuillerability Ty	Denial of Servic					_			เกษาเกลเเบ	11, 003-

Vulnerability Type(s)	Publish Date	cvss	De	escription	n & CVE	ID	Pa	tch	NCIII	PC ID
			the serv	ver and	cause a	denial				
			of servi	ce (DoS) condi	tion on				
			the affe	cted sys	stem. T	he				
			vulnera	bility is	due to					
			incomp	lete use	r-supp	lied				
			input va	alidatio	n when	a				
			custom	extensi	on atte	mpts				
			to chan	ge a DH	CPv6 p	acket				
			receive	d by the	applic	ation.				
			An atta	cker cou	ıld exp	loit				
			this vul	nerabili	ty by s	ending				
			malforr	ned DH	CPv6 p	ackets				
			to the a	pplicati	on. An	exploit				
			could a			_				
			trigger	a restar	t of the	<u> </u>				
			service	which,	if explo	ited				
			repeate	edly, mig	ght leac	l to a				
			DoS cor							
			vulnera	ability ca	an only	be				
			exploite	-	-					
			adminis			erver				
			has pre	viously	installe	ed				
			custom	_						
			attemp	t to mod	lify the	packet				
			details		-	-				
			been pr		•					
			Althoug							
			matche	-						
			been lo	U	•					
			because							
			only aff							
			that has							
			extensi			•				
			to modi			•				
					•					
			before the packet has been							
			completely sanitized. If							
			packet modification in a custom extension happens							
			after th		-	-				
CV Scoring Scale	9 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross									

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID				Pa	tch	NCII	PC ID
			will n vulne versio	zed, the ot be aff rability. ons prion are affe	ected by Softwar to 8.3(
				D : CVE-		840				
firepower_ma	 anagement_ce	enter								
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	3.5	based of Cisc Manage could auther attack site so agains based of an avulne insuff user-sweb-kinterf system explorate could executing the interfect of the could executing the interfect of the could executing the could execut in the could executing the could execut in the could execut in the could execute the could execut in the could execute the could execu	nerability manage affected rability icient vasce of the manage affected rability icient vasce of the m. An attact this vuading a table contain the arbitrace or acceptable one 6.2.3 are affected one 6.2.3 are affected one contain the context acceptable one 6.2.3 are affected one contain the context acceptable one 6.2.3 are affected one contain the context acceptable one 6.2.3 are affected one contain the context acceptable one context acceptable on context acceptable one context acceptable one context acceptable on context acceptable one context acceptable on con	ement in ower Center (, remote onduct a (XSS) at of the venent in system. is due to alidation input ir anagement and the affector acker could be affector acker to a cessful of the access send information of the access send informatic access send inf	FMC) cross- tack veb- terface The of the ed ould lity by access a licious exploit cer to pt code ffected nsitive, nation.	N/A		A-CIS- 01052	FIRE- 19/31
identity_serv	ices_engine									
CV Scoring Sca (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	17-04-2019	7.8	A vulnerability in the web interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to trigger high CPU usage, resulting in a denial of service (DoS) condition. The vulnerability is due to improper handling of Secure Sockets Layer (SSL) renegotiation requests. An attacker could exploit this vulnerability by sending renegotiation requests at a high rate. An successful exploit could increase the resource usage on the system, eventually leading to a DoS condition. This vulnerability affects version 2.1. CVE ID: CVE-2019-1718	N/A	A-CIS-IDEN- 010519/32
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	3.5	A vulnerability in the webbased guest portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a crosssite scripting (XSS) attack against a user of the webbased management interface. The vulnerability is due to insufficient validation of user-supplied input that is processed by the web-based interface. An attacker could exploit this vulnerability by persuading	N/A	A-CIS-IDEN- 010519/33

Vulnerability Type(s)	Publish Date	cvss	ı	Descriptio	on & CVE	ID	Pa	tch	NCII	PC ID
			click a success allow arbitr contest access based softwar	of the in crafted ssful exp the atta ary scrip at of the s sensitivity informated. D: CVE-	link. A oloit cou cker to e ot code i interfac we brow ation. Ci: ion 2.1 i	ld execute n the ce or ser- sco ISE s				
meeting_serv	er									
Uncontrolled Search Path Element	17-04-2019	3.6	path path path path path path path path	A vulnerability in the search path processing of Cisco Directory Connector could allow an authenticated, local attacker to load a binary of their choosing. The vulnerability is due to uncontrolled search path elements. An attacker could exploit this vulnerability by placing a binary of their choosing earlier in the search path utilized by Cisco Directory Connector to locate and load required resources. CVE ID: CVE-2019-1794		N/A		A-CIS- 01051	MEET- .9/34	
telepresence_	video_comm	unicati	on_ser	ver						
Improper Input Validation	17-04-2019	6.8	A vulnerability in the XML API of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote			N/A		A-CIS- 01051		
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause the CPU to increase to 100% utilization, causing a denial of service (DoS) condition on an affected system. The vulnerability is due to improper handling of the XML input. An attacker could exploit this vulnerability by sending a specifically crafted XML payload. A successful exploit could allow the attacker to exhaust CPU resources, resulting in a DoS condition until the system is manually rebooted. Software versions prior to X12.5.1 are affected. CVE ID: CVE-2019-1720		
N/A	17-04-2019	6.8	A vulnerability in the phone book feature of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker to cause the CPU to increase to 100% utilization, causing a denial of service (DoS) condition on an affected system. The vulnerability is due to improper handling of the XML input. An attacker could exploit this vulnerability by sending a Session Initiation Protocol (SIP) message with a crafted XML payload to an	N/A	A-CIS-TELE- 010519/36

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to exhaust CPU resources, resulting in a DoS condition. Manual intervention may be required to recover the device. This vulnerability is fixed in Cisco Expressway Series and Cisco TelePresence Video Communication Server Releases X12.5.1 and later.		
Cross-Site Request Forgery (CSRF)	17-04-2019	4.3	A vulnerability in the FindMe feature of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an unauthenticated, remote attacker to conduct a cross- site request forgery (CSRF) attack and perform arbitrary actions on an affected system. The vulnerability is due to insufficient CSRF protections for the web- based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to follow a maliciously crafted link. A successful exploit could allow the attacker to perform arbitrary actions on an affected system with the	N/A	A-CIS-TELE- 010519/37

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			privileges of the user. The arbitrary actions include adding an attacker-controlled device and redirecting calls intended for a specific user. For more information about CSRF attacks and potential mitigations, see Understanding Cross-Site Request Forgery Threat Vectors. This vulnerability is fixed in software version X12.5.1 and later.		
Cloudbees			CVE ID : CVE-2019-1722		
jenkins_opera	ntions center				
N/A	19-04-2019	5	CloudBees Jenkins Operations Center 2.150.2.3, when an expired trial license exists, allows Cleartext Password Storage and Retrieval via the proxy configuration page. CVE ID: CVE-2019-11350		A-CLO-JENK- 010519/38
cloudfoundry					
capi-release					
Improper Authenticati on	17-04-2019	6	Cloud Foundry Cloud Controller API Release, versions prior to 1.79.0, contains improper authentication when validating user permissions. A remote authenticated malicious user with the ability to create UAA clients	https://www .cloudfoundr y.org/blog/c ve-2019- 3798	A-CLO-CAPI- 010519/39
CV Scoring Scal (CVSS) Vulnerability Tv	0-1	1-2 Site Reg	2-3 3-4 4-5 5-6 uest Forgery; Dir. Trav Directory Tra	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss	1	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			of a vinay e to that creati equal victin	nowledgictim in escalate state of the magaclie to the gar. D: CVE-	the foun their pri victim b ent with uid of th	dation vileges y a name leir				
Clusterlabs										
pacemaker										
Use After Free	18-04-2019	5	found and ir which sensit leaked	-after-fr l in pace ncluding n could r cive info d via the D : CVE-	maker uversion esult in rmation system	2.0.1 certain to be logs.	N/A		A-CLU PACE- 01051	
Cmsmadesim	ple									
cms_made_sii										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	24-04-2019	3.5	Made has R "New Renar	ile Mana Simple eflected name" f ne actio D : CVE -	through XSS via ield in a n.	2.2.10 the	N/A		A-CMS CMS 01051	
Contao										
contao_cms										
Weak Password Recovery Mechanism for Forgotten Password	17-04-2019	5	before 4.7.3 has a Weak Password Recovery Mechanism for a Forgotten Password				o.org/ ws/se	curity- ability- 119-	A-CON CONT- 01051	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_				_			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10641		
Cross-Site Request Forgery (CSRF)	17-04-2019	6.8	Contao 4.7 allows CSRF. CVE ID : CVE-2019-10642	https://conta o.org/en/ne ws/security- vulnerability- cve-2019- 10642.html	A-CON- CONT- 010519/43
N/A	17-04-2019	7.5	Contao 4.7 allows Use of a Key Past its Expiration Date. CVE ID: CVE-2019-10643	https://conta o.org/en/ne ws/security- vulnerability- cve-2019- 10643.html	A-CON- CONT- 010519/44
Cutephp					
cutenews					
Unrestricted Upload of File with Dangerous Type	22-04-2019	6.5	An issue was discovered in CutePHP CuteNews 2.1.2. An attacker can infiltrate the server through the avatar upload process in the profile area via the avatar_file field to index.php?mod=main&opt=personal. There is no effective control of \$imgsize in /core/modules/dashboard.php. The header content of a file can be changed and the control can be bypassed for code execution. (An attacker can use the GIF header for this.) CVE ID: CVE-2019-11447	N/A	A-CUT- CUTE- 010519/45
datools					
daviewindy					
CV Scoring Scal	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Ty		_	uest Forgery; Dir. Trav Directory Travoss Site Scripting; Sql- SQL Injection; N 25		itormation; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-04-2019	6.8	DaviewIndy 8.98.7 and earlier versions have a Heapbased overflow vulnerability, triggered when the user opens a malformed DIB format file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. CVE ID: CVE-2019-9135	N/A	A-DAT- DAVI- 010519/46	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-04-2019	6.8	DaviewIndy 8.98.7 and earlier versions have a Heapbased overflow vulnerability, triggered when the user opens a malformed JPEG2000 format file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. CVE ID: CVE-2019-9136	N/A	A-DAT- DAVI- 010519/47	
Integer Overflow or Wraparound	25-04-2019	6.8	DaviewIndy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed PhotoShop file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. CVE ID: CVE-2019-9138	N/A	A-DAT- DAVI- 010519/48	
Integer Overflow or Wraparound	25-04-2019	6.8	DaviewIndy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered	N/A	A-DAT- DAVI- 010519/49	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			malfo misha Attacl and an execu	the user rmed PI andled by kers courbitrary tion.	DF file the property of the pr	nat is w.exe. it this				
Dell										
emc_isilonsd_	management	_serve	r							
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	4.3	1.1.0 c script uploa remot admir explos execu JavaSc contes	SD Mana contains ing vuln ding an te attack n user to it this vute malic cript cooxt of the D: CVE-	a cross erability OVA file er can to potential nerabilious HT le in the admin	site y while A rick an fally lity to ML or user.	N/A		A-DEI EMC 01051	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	4.3	1.1.0 c script regist A rem an add explose execu JavaSo contes	SD Mana contains vuln vering vC note atta min user it this vute malic cript cooxt of the D : CVE-	a cross erability enter so cker car to pote ilnerabilious HT le in the admin	site y while ervers. n trick entially lity to ML or user.	N/A		A-DEI EMC 01051	
supportassist										
Cross-Site Request Forgery	18-04-2019	6.8	Dell SupportAssist Client versions prior to 3.2.0.90 contain an improper origin validation vulnerability. An				N/A		A-DEI SUPP- 01051	
(CVSS)	CV Scoring Scale (CVSS) O-1 1-2 2-3 3-4 4-5 5-6 Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory T							7-8 fo- Gain Ir	8-9	9-10 n: DoS-
vuinerability Ty	pe(s): CSRF- Cross Denial of Service	_				_			nformatio	n; D0S-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			unauthenticated remote attacker could potentially exploit this vulnerability to attempt CSRF attacks on users of the impacted systems. CVE ID: CVE-2019-3718		
Improper Input Validation	18-04-2019	7.9	Dell SupportAssist Client versions prior to 3.2.0.90 contain a remote code execution vulnerability. An unauthenticated attacker, sharing the network access layer with the vulnerable system, can compromise the vulnerable system by tricking a victim user into downloading and executing arbitrary executables via SupportAssist client from attacker hosted sites. CVE ID: CVE-2019-3719	N/A	A-DEL- SUPP- 010519/53
deltaww	moditor				
cncsoft_scree	eneumor		Dolto Industrial Automotion	I	
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-04-2019	6.8	Delta Industrial Automation CNCSoft, CNCSoft ScreenEditor Version 1.00.88 and prior. Multiple stack-based buffer overflow vulnerabilities may be exploited by processing specially crafted project files, allowing an attacker to remotely execute arbitrary code. This may occur because CNCSoft lacks user input validation before	N/A	A-DEL- CNCS- 010519/54
				<u> </u>	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS	Descr	iption & CVE	ID	Pa	tch	NCIII	PC ID
			files onto t	ata from pro the stack. VE-2019-1					
Out-of- bounds Read	17-04-2019	4.3	Delta Industrial Automation CNCSoft, CNCSoft ScreenEditor Version 1.00.88 and prior. Multiple out-of-bounds read vulnerabilities may be exploited, allowing information disclosure due to a lack of user input validation for processing specially crafted project files. CVE ID: CVE-2019-10949 Delta Industrial Automation		N/A		A-DEL CNCS- 01051		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-04-2019	6.8	Delta Industrial Automation CNCSoft, CNCSoft ScreenEditor Version 1.00.88 and prior. Multiple heap-based buffer overflow vulnerabilities may be exploited by processing		N/A		A-DEL CNCS- 01051		
Drupal									
drupal									
Improper Neutralizatio n of Input During Web	19-04-2019	4.3	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles		N/A		A-DRU DRUP- 01051		
CV Scoring Scale (CVSS)	e 0-1 pe(s): CSRF- Cross	1-2	2-3 3-4		5-6	6-7	7-8	8-9	9-10

		because pollution source enumer proper native (e of Obon. If an object rable _ ty, it co	l(true, {} ject.prot n unsani containe _proto ould exte prototyp	totype tized ed an end the oe.				
		The clie				Ī			
		The clie							
		The clie							
019 6	6.8	Window injection parame handler escape Angular achieve executi origin2 for QtA QDeskt commu	rigin 10 ws allows allowed in the eter of the eter of the eter of the eter of the eter on via a serion via a	the Orig can be u derlying dbox an te code an ne/launo tion vices	in2 URI sed to d	N/A		A-EA-0 01051	
)19 4	4.3	In Eclipse Jetty version 9.2.26 and older, 9.3.25 and older, and 9.4.15 and older, the server is vulnerable to XSS conditions if a remote client USES a specially formatted URL against the DefaultServlet or ResourceHandler that is				eclipse ugs/sh		A-ECL 01051	•
	L-2	2-3 uest Forge	3-4 ery; Dir. T	4-5	5-6	6-7 ersal; +In	7-8 fo- Gain In	8-9	9-10 n; DoS-
(1-2 - Cross Site Req	client U format Default Resour 1-2 2-3 Cross Site Request Forge	client USES a formatted UR DefaultServle ResourceHand	client USES a specially formatted URL agains DefaultServlet or ResourceHandler that 1-2 2-3 3-4 4-5 Cross Site Request Forgery; Dir. Trav Directions in a Tensor Control of the Contro	client USES a specially formatted URL against the DefaultServlet or ResourceHandler that is 1-2 2-3 3-4 4-5 5-6 Cross Site Request Forgery; Dir. Trav Directory Trav.	client USES a specially g.cgi?id 121 DefaultServlet or ResourceHandler that is 1-2 2-3 3-4 4-5 5-6 6-7 Cross Site Request Forgery; Dir. Trav Directory Traversal; +Inc	client USES a specially formatted URL against the DefaultServlet or ResourceHandler that is 1-2 2-3 3-4 4-5 5-6 6-7 7-8	XSS conditions if a remote client USES a specially formatted URL against the DefaultServlet or ResourceHandler that is 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
			Listin	gured for g of dire D : CVE -	ctory co	ntents.				
Fedoraprojec	it									
389_directory	y_server									
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-04-2019	5	1.4.1.1 by wo socke work 'ioblo Howe applie encry Conno are no into a and munaut could hangi hang result Service	In 389-ds-base up to version 1.4.1.2, requests are handled by workers threads. Each sockets will be waited by the worker for at most 'ioblocktimeout' seconds. However this timeout applies only for unencrypted requests. Connections using SSL/TLS are not taking this timeout into account during reads, and may hang longer. An unauthenticated attacker could repeatedly create hanging LDAP requests to hang all the workers, resulting in a Denial of Service. CVE ID: CVE-2019-3883					A-FEI 01051	0-389 19/60
Ffmpeg										
ffmpeg										
NULL Pointer Dereference	18-04-2019	6.8	libavcodec/hevcdec.c in FFmpeg 4.1.2 mishandles detection of duplicate first slices, which allows remote attackers to cause a denial of service (NULL pointer dereference and out-of-array access) or possibly have unspecified other impact via			N/A		A-FFM FFMP 01051	-	
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; Dos- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			crafted HEVC data.		
			CVE ID : CVE-2019-11338		
Out-of- bounds Read	18-04-2019	6.8	The studio profile decoder in libavcodec/mpeg4videodec. c in FFmpeg 4.0 before 4.0.4 and 4.1 before 4.1.2 allows remote attackers to cause a denial of service (out-of-array access) or possibly have unspecified other impact via crafted MPEG-4 video data. CVE ID: CVE-2019-11339	N/A	A-FFM- FFMP- 010519/62
Freeradius					
freeradius					
Improper Authenticati on	22-04-2019	7.5	FreeRADIUS before 3.0.19 does not prevent use of reflection for authentication spoofing, aka a "Dragonblood" issue, a similar issue to CVE-2019-9497.	N/A	A-FRE- FREE- 010519/63
			CVE ID : CVE-2019-11234		
Insufficient Verification of Data Authenticity	22-04-2019	7.5	FreeRADIUS before 3.0.19 mishandles the "each participant verifies that the received scalar is within a range, and that the received group element is a valid point on the curve being used" protection mechanism, aka a "Dragonblood" issue, a similar issue to CVE-2019-9498 and CVE-2019-9499. CVE ID: CVE-2019-11235	N/A	A-FRE- FREE- 010519/64

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1			J .	. 5	3 0	Ŭ,	, 0	U J	J 10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
gbraad					
gauth					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-04-2019	4.3	GAuth 0.9.9 beta has stored XSS that shows a popup repeatedly and discloses cookies. CVE ID: CVE-2019-11084	https://githu b.com/gbraa d/gauth/issu es/110	A-GBR- GAUT- 010519/65
gilacms					
gila_cms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-04-2019	4	core/classes/db_backup.php in Gila CMS 1.10.1 allows admin/db_backup?downloa d= absolute path traversal to read arbitrary files. CVE ID: CVE-2019-11515	N/A	A-GIL-GILA- 010519/66
Cross-Site Request Forgery (CSRF)	22-04-2019	6.8	Gila CMS 1.10.1 allows fm/save CSRF for executing arbitrary PHP code. CVE ID: CVE-2019-11456	N/A	A-GIL-GILA- 010519/67
Gitlab					
gitlab					
Improper Access Control	16-04-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 9.x, 10.x, and 11.x before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control. CVE ID: CVE-2019-7155	https://gitla b.com/gitlab- org/gitlab- ce/issues/42 726	A-GIT-GITL- 010519/68

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	17-04-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control. CVE ID: CVE-2019-9170	https://gitla b.com/gitlab- org/gitlab- ce/issues/51 971	A-GIT-GITL- 010519/69
Information Exposure	17-04-2019	4.3	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 1 of 5). CVE ID: CVE-2019-9171	https://gitla b.com/gitlab- org/gitlab- ce/issues/54 635	A-GIT-GITL- 010519/70
Information Exposure	17-04-2019	4.3	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 2 of 5).	https://gitla b.com/gitlab- org/gitlab- ce/issues/54 795	A-GIT-GITL- 010519/71
Server-Side Request Forgery (SSRF)	17-04-2019	7.5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows SSRF. CVE ID: CVE-2019-9174	https://gitla b.com/gitlab- org/gitlab- ce/issues/55 468	A-GIT-GITL- 010519/72
Information Exposure	17-04-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure	https://gitla b.com/gitlab- org/gitlab- ce/issues/52 524	A-GIT-GITL- 010519/73

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(issue 3 of 5).		
			CVE ID : CVE-2019-9175		
Cross-Site Request Forgery (CSRF)	17-04-2019	5.8	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows CSRF.	https://gitla b.com/gitlab- org/gitlab- ce/issues/55 664	A-GIT-GITL- 010519/74
			CVE ID : CVE-2019-9176		
Information Exposure	17-04-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 4 of 5).	https://gitla b.com/gitlab- org/gitlab- ce/issues/54 803	A-GIT-GITL- 010519/75
			CVE ID : CVE-2019-9178		
Information Exposure	17-04-2019	4.3	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 5 of 5).	https://gitla b.com/gitlab- org/gitlab- ce/issues/54 783	A-GIT-GITL- 010519/76
			CVE ID : CVE-2019-9179		
N/A	17-04-2019	7.5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. Its User Interface has a Misrepresentation of Critical Information. CVE ID: CVE-2019-9217	N/A	A-GIT-GITL- 010519/77
Improper	17-04-2019	4.3	An issue was discovered in	https://gitla	A-GIT-GITL-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Access Control			GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 2 of 5). CVE ID: CVE-2019-9219	b.com/gitlab- org/gitlab- ce/issues/54 159	010519/78
N/A	17-04-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Uncontrolled Resource Consumption. CVE ID: CVE-2019-9220	https://gitla b.com/gitlab- org/gitlab- ce/issues/55 653	A-GIT-GITL- 010519/79
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-04-2019	5.5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Insecure Permissions. CVE ID: CVE-2019-9222	https://gitla b.com/gitlab- org/gitlab- ce/issues/56 348	A-GIT-GITL- 010519/80
Information Exposure	17-04-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure. CVE ID: CVE-2019-9223	https://gitla b.com/gitlab- org/gitlab- ce/issues/50 334	A-GIT-GITL- 010519/81
Improper Access Control	17-04-2019	5	An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It	https://gitla b.com/gitlab- org/gitlab- ce/issues/54 789	A-GIT-GITL- 010519/82

Vulnerability Type(s)	Publish Date	cvss	Description	on & CVE ID	ı	Patch	NCII	PC ID
			has Incorrect A	Access Contro	ol			
			CVE ID : CVE-	2019-9224				
Improper Access Control	17-04-2019	5	An issue was of GitLab Communication Enterprise Ed 11.6.10, 11.7.3 and 11.8.x before has Incorrect (issue 5 of 5).	unity and ition before k before 11.7. fore 11.8.1. It Access Contro	https b.cor org/	s://gitla n/gitlab- gitlab- ssues/54	A-GIT- 01051	-GITL- .9/83
			CVE ID : CVE-	2019-9225				
Improper Access Control	17-04-2019	7.5	An issue was of GitLab Common Enterprise Educating from before 11.6.10 11.7.6, and 11 11.8.1. It has I Access Contro vulnerability to 2019-9732.	unity and ition 10.x 10.8) and 11 , 11.7.x before ncorrect l, a different	https://eb.com	s://gitla m/gitlab- gitlab- ssues/54	A-GIT- 01051	
			CVE ID : CVE-	2019-9756				
N/A	17-04-2019	6.4	An issue was of GitLab Communication Enterprise Edit 11.x before 11 before 11.7.6, before 11.8.1. Permissions. CVE ID: CVE-	unity and ition 10.x and 6.10, 11.7.x and 11.8.x It has Insecu	l N/A		A-GIT- 01051	
Gnome								
evince								
Access of Uninitialized Pointer	22-04-2019	4.3	The tiff_document_tiff_document_		N/A		A-GNO- EVIN- 010519/86	
CV Scoring Scal (CVSS)	0-1	1-2	2-3 3-4 uest Forgery; Dir. T	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Į.	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			docum GNOM 3.32.0 from TIFFR ed(), l memo proce image	nent bac IE Evinc I did not ReadRGE eading t ory use v ssing ce e files.	rtain TII	gh errors Orient ialized				
gnome-deskto	ор									
Improper Input Validation	22-04-2019	6.8	An issue was discovered in GNOME gnome-desktop 3.26, 3.28, and 3.30 prior to 3.30.2.2, and 3.32 prior to 3.32.1.1. A compromised thumbnailer may escape the bubblewrap sandbox used to confine thumbnailers by using the TIOCSTI ioctl to push characters into the input buffer of the thumbnailer's controlling terminal, allowing an attacker to escape the sandbox if the thumbnailer has a controlling terminal. This is due to improper filtering of the TIOCSTI ioctl on 64-bit systems, similar to CVE-2019-10063.				N/A		A-GNO GNOM 01051	[-
Google										
tensorflow NULL	24-04-2019	4.3	NULL	pointer	derefer	ence in	N/A		A-GOO)
						1			•	

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
Pointer Dereference			1.12.2	e Tenso 2 could c e via an	ause a d	lenial of			TENS- 01051	9/88
			CVE I	D : CVE-	2019-9	635				
Gradle										
enterprise										
N/A	22-04-2019	5	2018. did no	ndle Ente 5.3, Buil ot store t t in an e	d Cache the cred	Nodes entials	N/A	A-GRA ENTE- 01051		
			CVE I	D : CVE-	2019-1	1402				
N/A	22-04-2019	5	2018. would passw viewi sourc	In Gradle Enterprise before 2018.5.2, Build Cache Nodes would reflect the configured password back when viewing the HTML page source of the settings page.					A-GRA ENTE- 01051	
			CVE I	D : CVE-	2019-1	1403				
Graphicsmag										
graphicsmagi	ick									
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-04-2019	6.8	In GraphicsMagick from version 1.3.8 to 1.4 snapshot-20190403 Q8, there is a heap-based buffer overflow in the function WritePDBImage of coders/pdb.c, which allows an attacker to cause a denial of service or possibly have unspecified other impact via a crafted image file. This is related to MagickBitStreamMSBWrite in magick/bit_stream.c.				N/A		A-GRA GRAP- 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PCID
			CVE I	D : CVE-	2019-1	1505				
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-04-2019	6.8	versice snaps there overfl Write coder an att of ser unspead a craft relate Export magic	tRedQu k/expoi	to 1.4 90403 (p-based te functi BImage (which a cause a cossibly ther imp ge file. The	28, buffer on of allows denial have bact via his is	N/A		A-GRA GRAP- 01051	
Out-of- bounds Read	23-04-2019	4.3	coders/xwd.c in GraphicsMagick 1.3.31 allows attackers to cause a denial of service (out-of- bounds read and application crash) by crafting an XWD image file, a different vulnerability than CVE- 2019-11008 and CVE-2019- 11009. CVE ID: CVE-2019-11473				N/A		A-GRA GRAP- 01051	
Improper Input Validation	23-04-2019	4.3	coders/xwd.c in GraphicsMagick 1.3.31 allows attackers to cause a denial of service (floating- point exception and application crash) by crafting an XWD image file, a different vulnerability than CVE-2019-11008 and CVE- 2019-11009.			N/A		A-GRA- GRAP- 010519/94		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			CVE I	D : CVE-	2019-1	1474				
gstreamer_pr	oject									
gstreamer										
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-04-2019	6.8	GStreamer before 1.16.0 has a heap-based buffer overflow in the RTSP connection parser via a crafted response from a server, potentially allowing remote code execution. CVE ID: CVE-2019-9928					sa-	A-GST GSTR- 01051	
IBM										
sterling_b2b_	integrator									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-04-2019	3.5	Stand 6.0.0.1 cross- vulne embe- code i alterin functi leadin disclo sessio 15710		ion 6.0.0 erable to pting. To allows under the UI the tended cotential dentials and the tended cotentials and the tended c	0.0 and o his sers to Script us llly usted ID:	.ibm.co	docvie?uid=ib	A-IBM STER- 01051	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-04-2019	3.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 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			Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended https://ww .ibm.com/su pport/docv w.wss?uid= m10880591		om/su docvie uid=ib	A-IBM STER- 01051	
CV Scoring Scal (CVSS) Vulnerability Ty	0-1	1-2 Site Req	2-3 uest Forg	3-4 gery; Dir. 1	4-5 rav Dire	5-6	6-7 ersal; +In	7-8 fo- Gain Ir	8-9	9-10 n; DoS-
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			leading to credentials disclosure within a trusted session. IBM X-Force ID: 157108.		
			CVE ID : CVE-2019-4074		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-04-2019	3.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 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: 157109.		A-IBM- STER- 010519/98
			CVE ID: CVE-2019-4075		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-04-2019	3.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 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: 157110. CVE ID: CVE-2019-4076		A-IBM- STER- 010519/99
Improper			IBM Sterling B2B Integrator	https://www	A IDM
Neutralizatio n of Input During Web	25-04-2019	3.5	Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This	. , ,	A-IBM- STER- 010519/100
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
(CVSS)					

Vulnerability Type(s)	Publi	ish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
Page Generation ('Cross-site Scripting')				ember code i alteria functi leadir disclo session 15712		ary Javas eb UI the tended potential dentials chin a tru K-Force	Script us lly usted ID:	m1088	30591		
Information Exposure	25-04	4-2019	3.5	IBM S Stand 6.0.0.1 authe sensit inforr circur ID: 15	terling Fard Edit could a nticated ive docu nation u nstances 8401. D: CVE-	32B Inte ion 6.0.0 allow an user to iment nder un s. IBM X	grator 0.0 and obtain usual -Force	.ibm.co	docvie Puid=ib	A-IBM STER- 01051	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-0	4-2019	3.5	Stand 6.0.0.7 cross- vulne embe- code i alterin functi leadin disclo sessio 15842	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 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: 158414.				//www om/su docvie Puid=ib 80591	A-IBM STER- 01051	
Information Exposure	25-04	4-2019	4	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 could allow an authenticated user to view				https://www .ibm.com/su pport/docvie w.wss?uid=ib		STER- 010519/103	
CV Scoring Scal (CVSS)	e	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			process definition of a business process without permission. IBM X-Force ID: 159231.	m10880595	
			CVE ID : CVE-2019-4222		
content_navig	gator				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-04-2019	3.5	IBM Content Navigator 2.0.3 and 3.0CD 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: 155999.	https://www .ibm.com/su pport/docvie w.wss?uid=ib m10869046	A-IBM- CONT- 010519/104
			CVE ID : CVE-2019-4033		
URL Redirection to Untrusted Site ('Open Redirect')	25-04-2019	5.8	IBM Content Navigator 2.0.3 and 3.0CD could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 157654.	N/A	A-IBM- CONT- 010519/105
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
	pe(s): CSRF- Cross	Site Req	uest Forgery; Dir. Trav Directory Tra	versal; +Info- Gain Ir	formation; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID			ID	Pa	tch	NCII	PC ID							
			CVE I	D : CVE-	2019-4	092											
infosphere_in	formation_se	rver															
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-04-2019	3.5	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 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: 159464. CVE ID: CVE-2019-4238				.ibm.co	docvie Puid=ib		I-INFO- 19/106							
					2019-4	238											
infosphere_in	formation_se	rver_o															
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-04-2019	3.5	Serve vulne script allows arbitr the W intend poten credes a trus	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 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: 159464.			.ibm.co	docvie Puid=ib		I-INFO- 19/107							
idreamsoft																	
icms																	
Improper Neutralizatio n of Input During Web Page	22-04-2019	4.3	An XSS issue was discovered in app/admincp/template/ad mincp.header.php in idreamsoft iCMS 7.0.14 via			N/A			-ICMS- 19/108								
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10							
		_	_	-		_		Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.									

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			the admincp.php?app=contab parameter. CVE ID: CVE-2019-1142		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	22-04-2019	4.3	An XSS issue was discover in app/search/search.app.ph in idreamsoft iCMS 7.0.14 the public/api.php?app=searcq parameter. CVE ID: CVE-2019-1142	via N/A h	A-IDR-ICMS- 010519/109
i-librarian					
I,_librarian					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	19-04-2019	4.3	Cross-site scripting (XSS) vulnerability in display.ph in I, Librarian 4.10 allows remote attackers to inject arbitrary web script or HTML via the project parameter. CVE ID: CVE-2019-1135	N/A	A-I-L-I,_L- 010519/110
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	22-04-2019	4.3	I, Librarian 4.10 has XSS verthe export.php export_files parameter. CVE ID: CVE-2019-11428	S N/A	A-I-L-I,_L - 010519/111
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	22-04-2019	4.3	I, Librarian 4.10 has XSS verthe notes.php notes parameter. CVE ID: CVE-2019-1144	N/A	A-I-L-I,_L - 010519/112
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-	6 6-7 7-8	8-9 9-10
		_	uest Forgery; Dir. Trav Directory oss Site Scripting; Sql- SQL Injectio		

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
Scripting')										
Imagemagick										
imagemagick										
Uncontrolled Resource Consumption	23-04-2019	7.1	The cineon parsing component in ImageMagick 7.0.8-26 Q16 allows attackers to cause a denial-of-service (uncontrolled resource consumption) by crafting a Cineon image with an incorrect claimed image size. This occurs because ReadCINImage in coders/cin.c lacks a check for insufficient image data in a file. CVE ID: CVE-2019-11470				N/A		A-IMA IMAG- 01051	
Divide By Zero	23-04-2019	4.3	coder image Image allow denia zero e XWD heade	ReadXWDImage in coders/xwd.c in the XWD image parsing component of ImageMagick 7.0.8-41 Q16 allows attackers to cause a denial-of-service (divide-byzero error) by crafting an XWD image file in which the header indicates neither LSB first nor MSB first.					A-IMA IMAG- 01051	
Intel										
graphics_perf	formance_ana	lyzer								
N/A	17-04-2019	4.6	Insufficient path checking in the installation package for Intel(R) Graphics Performance Analyzer for Linux version 18.4 and before may allow an			https://www .intel.com/co ntent/www/ us/en/securi ty- center/advis		A-INT GRAP- 01051		
CV Scoring Scal (CVSS)	0-1	1-2 Site Reg	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
vanierasinty Ty	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.									

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable escalation of privilege via local access. CVE ID: CVE-2019-0158	ory/intel-sa- 00236.html	
Jenkins					
gitlab					
Cross-Site Request Forgery (CSRF)	18-04-2019	3.5	A cross-site request forgery vulnerability in Jenkins GitLab Plugin 1.5.11 and earlier in the GitLabConnectionConfig#do TestConnection form validation method allowed attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. CVE ID: CVE-2019-10300	N/A	A-JEN-GITL- 010519/116
N/A	18-04-2019	4	A missing permission check in Jenkins GitLab Plugin 1.5.11 and earlier in the GitLabConnectionConfig#do TestConnection form validation method allowed attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. CVE ID: CVE-2019-10301	N/A	A-JEN-GITL- 010519/117

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	itch	NCII	IPC ID		
jira-ext			l .									
N/A	18-04-2019	4	crede its glo on the they o users maste	and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system. CVE ID: CVE-2019-10302				and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system.			-	-JIRA- 19/118
azure_publish	nersettings c	redenti	als									
N/A	18-04-2019	4	Jenkins Azure PublisherSettings Credentials Plugin 1.2 and earlier stored credentials unencrypted in the credentials.xml file on the Jenkins master where they could be viewed by users with access to the master file system. CVE ID: CVE-2019-10303				N/A		A-JEN- AZUR- 010519/119			
xebialabs_xl_	deploy											
Cross-Site Request Forgery (CSRF)	18-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins XebiaLabs XL Deploy Plugin in the Credential#doValidateUserN amePassword form validation method allows attackers to initiate a connection to an attackerspecified server. CVE ID: CVE-2019-10304			vulnerability in Jenkins XebiaLabs XL Deploy Plugin in the Credential#doValidateUserN amePassword form validation method allows attackers to initiate a connection to an attacker- specified server.				-XEBI- 19/120		
N/A	18-04-2019	4		sing per kins Xel			N/A		A-JEN-XEBI-			
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_				-			nformatio	on; DoS-		

ontrack N/A 18-04 Jquery		Deploy Plugin in the Credential#doValidateUserN amePassword form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server.		010519/121
N/A 18-04		CVIT VD CVIT 0040 4000		
N/A 18-04		CVE ID : CVE-2019-10305		
Jquery	4-2019 6.5	A sandbox bypass vulnerability in Jenkins ontrack Plugin 3.4 and earlier allowed attackers with control over ontrack DSL definitions to execute arbitrary code on the Jenkins master JVM. CVE ID: CVE-2019-10306	N/A	A-JEN- ONTR- 010519/122
jquery				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	4-2019 4.3	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {},) because of Object.prototype pollution. If an unsanitized source object contained an enumerableproto property, it could extend the native Object.prototype. CVE ID: CVE-2019-11358	N/A	A-JQU-JQUE- 010519/123
Kubernetes				
kubernetes				

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
N/A	22-04-2019	4.3	In Kubernetes v1.12.0-v1.12.4 and v1.13.0, the rest.AnonymousClientConfig () method returns a copy of the provided config, with credentials removed (bearer token, username/password, and client certificate/key data). In the affected versions, rest.AnonymousClientConfig () did not effectively clear service account credentials loaded using rest.InClusterConfig() CVE ID: CVE-2019-11243				N/A KU		A-KUB KUBE- 01051	
Matrix										
sydent										
Improper Input Validation	19-04-2019	4.3	Syder misha restri on e-rallow enabl of pot behav an emon user@ d.exan user@	an email.utils.parseaddr call on user@bad.example.net@goo d.example.com returns the user@bad.example.net substring.		N/A		A-MAT SYDE- 01051		
mediaarea										
mediainfo										
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

(CVSS)

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	120-04-2019 43		An out-of-bounds read in MediaInfoLib::File_Tags_Hel per::Synched_Test in Tag/File_Tags.cpp in MediaInfoLib in MediaArea MediaInfo 18.12 leads to a crash. CVE ID: CVE-2019-11372	N/A	A-MED- MEDI- 010519/126
Out-of- bounds Read	20-04-2019	4.3	An out-of-bounds read in File_Analyze::Get_L8 in File_Analyze_Buffer.cpp in MediaInfoLib in MediaArea MediaInfo 18.12 leads to a crash. CVE ID: CVE-2019-11373	N/A	A-MED- MEDI- 010519/127
meisivod					
msvod					
Cross-Site Request Forgery (CSRF)	20-04-2019	4.3	Msvod v10 has a CSRF vulnerability to change user information via the admin/member/edit.html URI. CVE ID: CVE-2019-11375	N/A	A-MEI- MSVO- 010519/128
miniblog.core	e_project				
miniblog.core)				
Improper Input Validation	16-04-2019	7.5	madskristensen Miniblog.Core through 2019- 01-16 allows remote attackers to execute arbitrary ASPX code via an IMG element with a data: URL, because SaveFilesToDisk in Controllers/BlogController.c s writes a decoded base64	N/A	A-MIN-MINI- 010519/129

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			string to a file without validating the extension.		
			CVE ID : CVE-2019-9845		
mkcms_proje	ct			<u> </u>	-
mkcms					
Improper Authenticati on	18-04-2019	6.8	MKCMS 5.0 allows remote attackers to take over arbitrary user accounts by posting a username and email address to ucenter/repass.php, which triggers e-mail transmission with the password, as demonstrated by 123456.	N/A	A-MKC- MKCM- 010519/130
			CVE ID: CVE-2019-11332		
Modsecurity					
owasp_modse	ecurity_core_r	ule_set			_
Incorrect Regular Expression	20-04-2019	5	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with nested repetition operators.	N/A	A-MOD- OWAS- 010519/131
			CVE ID : CVE-2019-11387		
Incorrect Regular Expression	20-04-2019	5	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf allows remote	N/A	A-MOD- OWAS- 010519/132

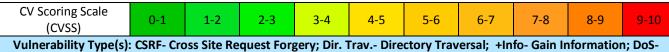
Vulnerability Type(s)	Publish Date	cvss	Description	on & CVE ID	Pat	ch	NCII	PC ID
				_				
			CVE ID : CVE-	2019-11388				
Incorrect Regular Expression	20-04-2019	5	/rules/REQUE APPLICATION PHP.conf allow attackers to ca	ecurity Core) through 3.1.0. EST-933ATTACK- ws remote ause a denial of (S) by entering fted string the beginning	N/A		A-MOI OWAS 01051	
			CVE ID : CVE-	2019-11389				
Incorrect Regular Expression	20-04-2019	5	An issue was of OWASP ModS Rule Set (CRS) /rules/REQUE APPLICATION PHP.conf allow attackers to caservice (ReDO a specially crawith set_error the beginning repetition oper CVE ID : CVE-	N/A		A-MOI OWAS 01051		
Incorrect Regular Expression	20-04-2019	5	OWASP ModS	·			A-MOI OWAS 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & (CVE ID	Pat	tch	NCII	PC ID
			PHP.conf allows reattackers to cause service (ReDOS) by a specially crafted with \$a# at the begand nested repetition operators.					
Mozilla			CVE ID : CVE-2019					
firefox								
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-04-2019	7.5	Mozilla developers community member reported memory bugs present in Fir Firefox ESR 60.5, a Thunderbird 60.5. these bugs showed of memory corrupt we presume that we enough effort that these could be exprunarbitrary code vulnerability affect Thunderbird < 60. ESR < 60.6, and Firefox ESR < 60.6, and Firefox EVE ID : CVE-2019	ers safety refox 65, nd Some of l evidence tion and with some of loited to . This es 6, Firefox refox < 66.	N/A		A-MO: FIRE- 01051	Z- .9/136
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-04-2019	7.5	Mozilla developers community member reported memory bugs present in Fir Some of these bugs evidence of memory corruption and we that with enough esome of these coulexploited to run arcode. This vulneral	N/A		A-MO: FIRE- 01051	Z- .9/137	
CV Scoring Scal	le 0-1	1-2	2-3 3-4 4-5	5 5-6	6-7	7-8	8-9	9-10
	pe(s): CSRF- Cross	Site Req	uest Forgery; Dir. Trav I	Directory Trav	ersal; +Inf	o- Gain I	nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			affects Firefox < 66.		
			CVE ID : CVE-2019-9789		
Use After Free	26-04-2019	7.5	A use-after-free vulnerability can occur when a raw pointer to a DOM element on a page is obtained using JavaScript and the element is then removed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	N/A	A-MOZ- FIRE- 010519/138
			CVE ID : CVE-2019-9790		
firefox_esr					
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-04-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 65, Firefox ESR 60.5, and Thunderbird 60.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	N/A	A-MOZ- FIRE- 010519/139
Use After Free	26-04-2019	7.5	A use-after-free vulnerability can occur when a raw pointer to a DOM element on a page is obtained using JavaScript and the element is	N/A	A-MOZ- FIRE- 010519/140

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			then removed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.		
			CVE ID: CVE-2019-9790		
thunderbird					
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-04-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 65, Firefox ESR 60.5, and Thunderbird 60.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	N/A	A-MOZ- THUN- 010519/141
			CVE ID: CVE-2019-9788		
Use After Free	26-04-2019	7.5	A use-after-free vulnerability can occur when a raw pointer to a DOM element on a page is obtained using JavaScript and the element is then removed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	N/A	A-MOZ- THUN- 010519/142

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Nice					
engage					
N/A	23-04-2019	7.5	In NICE Engage through 6.5, the default configuration binds an unauthenticated JMX/RMI interface to all network interfaces, without restricting registration of MBeans, which allows remote attackers to execute arbitrary code via the RMI protocol by using the JMX connector. The observed affected TCP port is 6338 but, based on the product's configuration, a different one could be vulnerable. CVE ID: CVE-2019-7727	N/A	A-NIC- ENGA- 010519/143
Nmap					
npcap					
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-04-2019	9.3	An issue was discovered in Npcap 0.992. Sending a malformed .pcap file with the loopback adapter using either pcap_sendqueue_queue() or pcap_sendqueue_transmit() results in kernel pool corruption. This could lead to arbitrary code executing inside the Windows kernel and allow escalation of privileges. CVE ID: CVE-2019-11490	N/A	A-NMA- NPCA- 010519/144
NTP					



Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID			
ntp		_											
N/A	18-04-2019	7.5	5905, mode numb which remot off-pa	(NTP), as specified in RFC 5905, uses port 123 even for modes where a fixed port number is not required, which makes it easier for remote attackers to conduct off-path attacks. CVE ID: CVE-2019-11331						P-NTP- 9/145			
Openkm													
openkm													
Unrestricted Upload of File with Dangerous Type	22-04-2019	9	OpenKM 6.3.2 through 6.3.7 allows an attacker to upload a malicious JSP file into the /okm:root directories and move that file to the home directory of the site, via frontend/FileUpload and admin/repository_export.jsp. This is achieved by interfering with the Filesystem path control in the admin's Export field. As a result, attackers can gain remote code execution through the application server with root privileges.				N/A		A-OPE OPEN 01051				
Oracle													
mysql													
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are https://supp ort.f5.com/cs p/article/K5 8502649			A-ORA MYSQ 01051							
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10			
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_							nformatio	n; DoS-			

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).		
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector:	https://supp ort.f5.com/cs p/article/K5 8502649	A-ORA- MYSQ- 010519/148

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2580		
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://supp ort.f5.com/cs p/article/K5 8502649	A-ORA- MYSQ- 010519/149
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple	https://supp ort.f5.com/cs p/article/K5 8502649	A-ORA- MYSQ- 010519/150

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2584		
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2585	https://supp ort.f5.com/cs p/article/K5 4470776	A-ORA- MYSQ- 010519/151
Improper Access	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle	https://supp ort.f5.com/cs	A-ORA- MYSQ-

 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)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Control			MySQL (subcomponent: Server: Partition). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2587	p/article/K5 4470776	010519/152
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL	https://supp ort.f5.com/cs p/article/K5 4470776	A-ORA- MYSQ- 010519/153

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2589		
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2592	https://supp ort.f5.com/cs p/article/K5 4470776	A-ORA- MYSQ- 010519/154
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with	https://supp ort.f5.com/cs p/article/K5 4470776	A-ORA- MYSQ- 010519/155

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).		
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2596	https://supp ort.f5.com/cs p/article/K5 2514501	A-ORA- MYSQ- 010519/156

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2606	https://supp ort.f5.com/cs p/article/K5 2514501	A-ORA- MYSQ- 010519/157
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or	https://supp ort.f5.com/cs p/article/K5 2514501	A-ORA- MYSQ- 010519/158

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2607		
Improper Access Control	23-04-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H /UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2614	https://supp ort.f5.com/cs p/article/K5 2514501	A-ORA- MYSQ- 010519/159
Improper Input Validation	23-04-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are	https://supp ort.f5.com/cs p/article/K5 2514501	A-ORA- MYSQ- 010519/160

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).		
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector:	https://supp ort.f5.com/cs p/article/K4 3540241	A-ORA- MYSQ- 010519/161

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2620		
Improper Input Validation	23-04-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2623	https://supp ort.f5.com/cs p/article/K4 3540241	A-ORA- MYSQ- 010519/162
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	https://supp ort.f5.com/cs p/article/K4 3540241	A-ORA- MYSQ- 010519/163

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2624		
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2625	https://supp ort.f5.com/cs p/article/K4 3540241	A-ORA- MYSQ- 010519/164
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported	https://supp ort.f5.com/cs p/article/K4 3540241	A-ORA- MYSQ- 010519/165

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).		
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score	https://supp ort.f5.com/cs p/article/K3 2798641	A-ORA- MYSQ- 010519/166

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2627		
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2628	https://supp ort.f5.com/cs p/article/K3 2798641	A-ORA- MYSQ- 010519/167
Improper Input Validation	23-04-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with	https://supp ort.f5.com/cs p/article/K3 2798641	A-ORA- MYSQ- 010519/168

 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)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).		
			CVE ID: CVE-2019-2630		
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Information Schema). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H).	https://supp ort.f5.com/cs p/article/K3 2798641	A-ORA- MYSQ- 010519/169

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID					
			CVE I	D : CVE-	2019-2	631									
Improper Input Validation	23-04-2019	5	Serve MySQ Serve Suppo affect and 8 explo- allow attack access to cor Serve this v in una critica access access (Confi CVSS (CVSS UI:N/	rability r compose L (subcompose r: Plugg orted vere ed are 5 .0.15 and itable vur s unauth s via mu inpromis r. Success ulnerabi authoriz al data o s to all M sible dat Score 7.5 identiali Vector: 6:3.0/AV S:U/C:H D: CVE-	nent of omponer able Autorions the Total and prior. It is a metwork at the English at English	Oracle nt: th). nat are d prior Easily lity ed k cotocols L acks of result as to ete erver 3.0 cts).		•	A-ORA MYSQ 01051						
Improper Input Validation	23-04-2019	1.9	Serve MySQ Serve Suppo affect Diffict vulne unaut with I infras Serve	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server.		Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL		Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL		er component of Oracle QL (subcomponent: er: Replication). orted versions that are ted are 8.0.15 and prior. cult to exploit erability allows thenticated attacker logon to the structure where MySQL			-	A-ORA MYSQ 01051	
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10					
vuinerability Ty	pe(s): CSRF- Cross Denial of Service	_				_			irormatio	on; DOS-					

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2634		
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2635	https://supp ort.f5.com/cs p/article/K4 2793451	A-ORA- MYSQ- 010519/172
Improper	23-04-2019	3.5	Vulnerability in the MySQL	https://supp	A-ORA-
Input			Server component of Oracle	ort.f5.com/cs	MYSQ-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Validation			MySQL (subcomponent: Server: Group Replication Plugin). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via MySQL Procotol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H /UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2636	p/article/K4 2793451	010519/173
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS	https://supp ort.f5.com/cs p/article/K4 2793451	A-ORA- MYSQ- 010519/174

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2644		
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2681	https://supp ort.f5.com/cs p/article/K4 2793451	A-ORA- MYSQ- 010519/175
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable	https://supp ort.f5.com/cs p/article/K2 8312671	A-ORA- MYSQ- 010519/176

Vulnerability Type(s)	Publish Date	cvss	Description	& CVE ID	Pat	tch	NCIII	PC ID
			UI:N/S:U/C:N/I:	ker with via multiple appromise Successful ulnerability authorized a hang or atable crash of MySQL Base Score impacts). /AC:L/PR:H/				
Improper Input Validation	23-04-2019	4	protocols to compromise MySQL Server. Successful		https:/ ort.f5.c p/artic 83126	com/cs cle/K2	A-ORA MYSQ- 01051	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & C	VE ID	Pat	tch	NCIII	PC ID
			CVE ID : CVE-2019	-2685				
Improper Input Validation	23-04-2019	4	Vulnerability in the Server component MySQL (subcomponent MySQL (subcomponent MySQL (subcomponent MySQL versions affected are 8.0.15). Easily exploitable vulnerability allow privileged attacker network access via protocols to component MySQL Server. Succeed attacks of this vulnerability to cause a harmonic of the server of	of Oracle nent: a that are and prior. a high with multiple omise cessful erability norized ang or ole crash MySQL se Score pacts). C:L/PR:H/A:H).	https:/ ort.f5.c p/artic 83126	com/cs cle/K2	A-ORA MYSQ- 01051	
Improper Input Validation	23-04-2019	4	Vulnerability in the Server component MySQL (subcompo Server: Optimizer). Supported versions affected are 8.0.15 Easily exploitable vulnerability allow privileged attacker network access via protocols to compre MySQL Server. Succentrally and attacks of this vulnerability in unaution result in unautions.	of Oracle nent: a that are and prior. s high with multiple omise cessful erability	https:/ ort.f5.c p/artic 83126	com/cs cle/K2	A-ORA MYSQ- 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2687		
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2688	https://supp ort.f5.com/cs p/article/K2 8312671	A-ORA- MYSQ- 010519/180
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are	https://supp ort.f5.com/cs p/article/K0 4246541	A-ORA- MYSQ- 010519/181

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2689		
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector:	https://supp ort.f5.com/cs p/article/K0 4246541	A-ORA- MYSQ- 010519/182

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2019-2691		
Improper Input Validation	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2693	https://supp ort.f5.com/cs p/article/K0 4246541	A-ORA- MYSQ- 010519/183
Improper Access Control	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise	https://supp ort.f5.com/cs p/article/K0 4246541	A-ORA- MYSQ- 010519/184

Vulnerability Type(s)	Publish D	oate CVS	Description & CVE ID MySQL Server. Successful				Pa	atch	NCII	PC ID
			attack can re ability frequ (comy Serve 6.5 (A CVSS (CVSS UI:N/	esult in usy to cause ently replete DO r. CVSS availabile Vector: S:3.0/AVS:U/C:N	e vulnera inautho se a hang beatable S) of My 3.0 Base ity impa :N/AC:L /I:N/A:I	ability rized g or crash rSQL Score cts). /PR:L/ H).				
Improper Input Validation	23-04-20	019 4	Vulne Serve MySQ Serve Suppo affect Easily vulne privil netwo proto MySQ attack can ro ability frequ (comp Serve 6.5 (A CVSS (CVSS UI:N/	UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2694 Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/ UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2695			ort.f5.	//supp com/cs cle/K0 541	A-ORA MYSQ 01053	
jdk			_						T	
Improper	23-04-20)19 5	Vulne	erability	in the Ja	va SE,	N/A		A-ORA	A-JDK-
CV Scoring Scal (CVSS)	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Access Control			Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). CVE ID: CVE-2019-2602		010519/186
Improper Access Control	23-04-2019	4.3	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 7u211,	N/A	A-ORA-JDK- 010519/187

(CVSS)	Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AN:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in Fava SE component of Oracle Java SE N/A A-ORA-JDK (010519/18)				8u202	2, 11.0.2	and 12;	Java				
vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access Data SE Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) O 1 12 2 3 34 4-5 5-6 6-7 7-8 8-9 5-1				SE En	nbedded	: 8u201					
unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AAV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 0.1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 5-1				Diffic	ult to ex	ploit					
with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in be Java SE component of Oracle Java SE Vulnerability in the Java SE CVS Corting Scale (CVSS) 3.4 4-5 5-6 6-7 7-8 8-9 9-1				vulne	rability	allows					
multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/:H/A:N). CVE ID: CVE-2019-2684 Improper Access Old 1.2 2.3 3.4 4.5 5.6 6.7 7.8 8.9 5.1				unaut	hentica	ed attac	cker				
compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID : CVE-2019-2684 Improper Access 0.1 0.1 0.2 0.3 0.4 0.7 0.8 0.9 0.9 0.9 0.9 0.9 0.9 0.9 0.9 0.9 0.9				with 1	network	access v	via				
Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE				multi	ple prot	ocols to					
attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access O-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1				_							
can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1											
creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1				1							
modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access O-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1							rized				
critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1					•						
Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1											
data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1				1							
applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1				1							
typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1											
sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE N/A A-ORA-JDK 010519/18											
applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1					-		_				
Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1					-						
that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1											
code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1				-		-	-				
from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1											
on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1											
security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1						-	-				
can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1					-						
using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 3-4 4-5 5-6 6-7 7-8 8-9 9-1					•		•				
Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1						•	•				
web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1				_		_					
data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1				•		•	Ŭ				
Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID : CVE-2019-2684											
impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N /UI:N/S:U/C:N/I:H/A:N). CVE ID: CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE (CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-18											
CVSS:3.0/AV:N/AC:H/PR:N							-				
CVE ID : CVE-2019-2684				-	-						
CVE ID : CVE-2019-2684 Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE N/A A-ORA-JDK-010519/18 CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1				`	•	•	•				
Improper Access 23-04-2019 6.8 Vulnerability in the Java SE component of Oracle Java SE N/A A-ORA-JDK-010519/18 CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1				,							
Access 23-04-2019 6.8 component of Oracle Java SE N/A 010519/18 CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1	Immusees									Δ-ΩR/	/-IDK-
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10		23-04-2019	6.8		-	-		N/A			•
	_	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS											

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pa	tch	NCII	PC ID
Control			(subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows				
			unauthenticated attacker with network access via multiple protocols to				
			compromise Java SE. Successful attacks of this				
			vulnerability can result in takeover of Java SE. Note: This vulnerability applies to				
			Java deployments, typically in clients running sandboxed				
			Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and				
			run untrusted code (e.g., code that comes from the				
			internet) and rely on the Java sandbox for security. This vulnerability does not				
			apply to Java deployments, typically in servers, that load				
			and run only trusted code (e.g., code installed by an administrator). CVSS 3.0				
			Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N				
			/UI:N/S:U/C:H/I:H/A:H). CVE ID : CVE-2019-2697				
Improper Access	23-04-2019	6.8	Vulnerability in the Java SE component of Oracle Java SE	N/A			A-JDK-
Control			(subcomponent: 2D).	,		01051	19/189
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
		_	uest Forgery; Dir. Trav Directory Tra oss Site Scripting; Sql- SQL Injection;				on; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			affection and 8 explored in composition with a multiple composition of the second in clies and a second in code at the second in cod	orted vered are January verof	ava SE: 7 ifficult to rability a ted attace access to ocols to ava SE. N oility app ents, typ ning san of applica Java applica Java applica Java applica I code (e nes from rely on for secu oility doe deploym rvers, th trusted of talled by c). CVSS 1 ty, Integ ty impact	dilows cker dilows cker dia chis dit in ote: olies to olically dboxed ations plets d and c.g., the rity. es not nents, nat load code dian 3.0 grity cts).				
			CVE I	D : CVE-	2019-2	698				
Improper Access Control	23-04-2019	6.8	comp (subc	rability onent of ompone The sup	Oracle nt: Wind	Java SE dows	ort.f5.	//supp com/cs cle/K0 14	A-ORA 01051	A-JDK- .9/190
CV Scoring Scale (CVSS) Vulnerability Typ	0-1 De(s): CSRF- Cross Denial of Service	_				_			8-9 nformatio	9-10 n; DoS-

Vulnerability Type(s)	Publish Date	cvss	ſ	Description	on & CVE	ID	Pa	tch	NCIII	PC ID		
			su202 vulne unaut with r multip composition SE, att impact Succe vulne takeo This v Java d in clie Java V or san (in Java run un code t intern Java s This v be exp the sp e.g., th which APIs. (Confi and A CVSS (CVSS /UI:N)	s affected 2. Difficult rability is thenticated by the protogram of Jacks makes and and box of the ployments rund and box of the ployments and box of the ployments of the ployments of the ployments rund and box of the ployments of the ployments and box of the ployments of the ployments and box of the ployments of	alt to expallows allows and attack of the can result of the can rely on	while Java icantly ducts. chis dit in ote: olies to olically dboxed ations plets ad and e.g., the the rity. also APIs in ent, rvice o the core 9.0 grity cts). I/PR:N :H).						
outside_in_ted	chnology		CVE	D. CVE	2017-2							
Improper Access	23-04-2019	7.5		rability de In Te			N/A		A-ORA			
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10												
vuinerability Ty	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; Dos- Denial of Service; XSS- Cross Site Scripting; SqI- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE	ID	Pat	tch	NCIII	PC ID
Control			component c	f Oracle I	usion			01051	9/191
			Middleware	(subcomp	onent:				
			Outside In Fi	lters).					
			Supported ve	ersions th	at are				
			affected are 8	3.5.3 and	8.5.4.				
			Easily exploi	table					
			vulnerability	allows					
			unauthentica	ited attac	ker				
			with networl	c access v	ria				
			HTTP to com	promise	Oracle				
			Outside In Te	chnology	7.				
			Successful at	tacks of t	his				
			vulnerability	can resu	lt in				
			unauthorized						
			or delete acc	-					
			Oracle Outsid	le In					
			Technology a	ccessible	data				
			as well as un						
			access to a su	bset of O	racle				
			Outside In Te						
			accessible da	0.0					
			unauthorized		o cause				
			a partial den	_					
			(partial DOS)						
			Outside In Te						
			Outside In Te						
			suite of softw		15 4				
			development		(c)				
			The protocol						
			depend on th						
			uses the Outs		c mat				
					CUCC				
			Technology of score assume						
					C				
			software pas received ove		rdr				
					ıĸ				
			directly to O		if data				
			Technology of		n uata				
			is not receive network the		re mav				
CV Scoring Scal	e								
(CVSS)	0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:N/S:U/C:L/I:L/A:L). CVE ID: CVE-2019-2608		
Improper Access Control	23-04-2019	6.4	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data	N/A	A-ORA- OUTS- 010519/192

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L). CVE ID: CVE-2019-2609		
Improper Access Control	23-04-2019	6.4	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and	N/A	A-ORA- OUTS- 010519/193

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).		
			CVE ID : CVE-2019-2610		
Improper Access Control	23-04-2019	6.4	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of	N/A	A-ORA- OUTS- 010519/194

CV Scoring Scale (CVSS)

O-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoSDenial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:N/S:U/C:L/I:N/A:L).		
Improper Access Control	23-04-2019	6.4	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to	N/A	A-ORA- OUTS- 010519/195

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).		
Improper Access Control	23-04-2019	6.4	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via	N/A	A-ORA- OUTS- 010519/196

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:N/S:U/C:L/I:N/A:L).		
Improper Access Control	23-04-2019	6.4	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are	N/A	A-ORA- OUTS- 010519/197

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			affected are 8.5.3 and 8.5.4.		
			Easily exploitable		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			HTTP to compromise Oracle		
			Outside In Technology.		
			Successful attacks of this		
			vulnerability can result in		
			unauthorized ability to cause		
			a hang or frequently		
			repeatable crash (complete		
			DOS) of Oracle Outside In		
			Technology as well as		
			unauthorized update, insert		
			or delete access to some of		
			Oracle Outside In		
			Technology accessible data.		
			Note: Outside In Technology		
			is a suite of software		
			development kits (SDKs).		
			The protocol and CVSS score		
			depend on the software that		
			uses the Outside In		
			Technology code. The CVSS		
			score assumes that the		
			software passes data		
			received over a network		
			directly to Outside In		
			Technology code, but if data		
			is not received over a		
			network the CVSS score may		
			be lower. CVSS 3.0 Base		
			Score 8.2 (Integrity and		
			Availability impacts). CVSS		
			Vector:		
			(CVSS:3.0/AV:N/AC:L/PR:N/		
			UI:N/S:U/C:N/I:L/A:H).		
			, , , , ,		

CV Scoring Scale (CVSS)

O-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2705		
vm_virtualbo	x				
Improper Access Control	23-04-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	N/A	A-ORA- VM_V- 010519/198
Improper Input Validation	23-04-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are	N/A	A-ORA- VM_V- 010519/199

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/ UI:N/S:C/C:H/I:H/A:H). CVE ID: CVE-2019-2656		
Improper Input Validation	23-04-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability	N/A	A-ORA- VM_V- 010519/200

Vulnerability Type(s)	Publish Date	cvss	Descri	ption & CVE	ID	Pa	tch	NCIII	PC ID
			can result in Oracle VM 3.0 Base So (Confident and Availal CVSS Vector (CVSS:3.0/UI:N/S:U/CCVE ID : CVE	VirtualBox ore 7.8 iality, Integoility impacor: AV:L/AC:L C:H/I:H/A:I	. CVSS grity cts). /PR:L/ H).				
Improper Access Control	23-04-2019	2.1	Vulnerability VM Virtual Oracle Virtual Oracle Virtual Comported affected are and prior the exploitable allows low attacker with infrastruct VM Virtual Compromis Virtual Box vulnerability Virtual Box significant additional Successful vulnerability unauthorize critical data access to a Virtual Box CVSS 3.0 B (Confident CVSS Vector (CVSS:3.0/UI:N/S:C/C	N/A		A-ORA VM_V- 01051			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Pul	olish Date	cvss	ı	Description	on & CVE	ID	Pa	atch	NCII	PC ID
				CVE I	D : CVE-	2019-2	678				
Improper Input Validation	23-	04-2019	3.6	VM Vi Oracle (subce Support affects and p explose allows attack infras VM Vi comp Virtua vulne Virtua signifi additi Succe vulne unaut a hang repea DOS) Virtua read a Oracle access Base S (Confi Availa Vecto (CVSS UI:N/	e Virtual ompone orted vered are Prior to 6 itable vusto itable vusto itable vusto itable vusto itable vusto itable vusto itablity itable vusto itab	x composization nt: Core rsions the rior to 5 .0.6. East linerability leged logon to execut Oracle Value the tacks manact oducts. acks of to can resurability to a subsect logon to execut of the conference of th	onent of o). nat are 5.2.28 sily lity o the Oracle tes to M acle VM ay chis alt in to cause horized et of 5.3.0 CVSS /PR:L/I).	N/A		A-OR/ VM_V- 01051	
Improper Input	23-	04-2019	4.6	Vulnerability in the Oracle				N/A		A-ORA VM V-	
CV Scoring Sca	le l		1-2	VM VirtualBox component of 2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Validation			Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). CVE ID: CVE-2019-2680		010519/203
Improper Access Control	23-04-2019	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise	N/A	A-ORA- VM_V- 010519/204

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).		
			CVE ID : CVE-2019-2690 Vulnerability in the Oracle		
Improper Access Control	23-04-2019	CVE ID: CVE-2019-2690 Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle		N/A	A-ORA- VM_V- 010519/205

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).		
			CVE ID : CVE-2019-2696		
Improper Input Validation	23-04-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/ UI:N/S:C/C:H/I:H/A:H). CVE ID: CVE-2019-2703	N/A	A-ORA- VM_V- 010519/206
Improper Input Validation	23-04-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core).	N/A	A-ORA- VM_V- 010519/207

 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)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).		
Improper Input Validation	23-04-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the	N/A	A-ORA- VM_V- 010519/208

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/ UI:N/S:C/C:H/I:H/A:H). CVE ID: CVE-2019-2722		
Improper Input Validation	23-04-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability	N/A	A-ORA- VM_V- 010519/209

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pato	ch	NCIII	PCID
			impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/ UI:N/S:C/C:H/I:H/A:H).				
			CVE ID : CVE-2019-2723				
transportatio	n_manageme	nt					
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Transportation Management component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 6.3.7, 6.4.2 and 6.4.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Transportation Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.0 Base Score 6.1	N/A		A-ORA TRAN- 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
<u> </u>		_	uest Forgery; Dir. Trav Directory Tra oss Site Scripting; Sql- SQL Injection; I 106			nformatio	n; DoS-

attacks of this vulnerability	Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). The supported version that is affected is 18.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability Vulnerability in the Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability				Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).		
Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). The supported version that is affected is 18.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability	primavera_p6	5_enterprise_p	project	_portfolio_management		
read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-2701	Access		4	Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). The supported version that is affected is 18.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/ UI:N/S:U/C:L/I:N/A:N).	N/A	

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): CSRE, Cross Site Request Forgery: Dir, Tray - Directory Trayersal: +Info- Gain Information: DoS-										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	23-04-2019	4.6	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Grid Infrastructure User privilege with logon to the infrastructure where Portable Clusterware executes to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Portable Clusterware. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/ UI:N/S:C/C:H/I:H/A:H). CVE ID: CVE-2019-2516	N/A	A-ORA- DATA- 010519/212
Improper Access Control	23-04-2019	7.5	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having DBFS_ROLE privilege with network	N/A	A-ORA- DATA- 010519/213

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	tch	NCIIP	C ID
			access via Oracle Net to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:DU:N/S:C/C:H/I:H/A:H).				
Improper Access Control	23-04-2019	6	Vulnerability in the Java VN component of Oracle Database Server. Supporte versions that are affected a 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR: UI:N/S:U/C:H/I:H/A:H).	d are		A-ORA- DATA- 010519	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2518		
N/A	23-04-2019	6	Vulnerability in the RDBMS DataPump component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Difficult to exploit vulnerability allows high privileged attacker having DBA role privilege with network access via Oracle Net to compromise RDBMS DataPump. Successful attacks of this vulnerability can result in takeover of RDBMS DataPump. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H /UI:N/S:U/C:H/I:H/A:H). CVE ID: CVE-2019-2571	N/A	A-ORA- DATA- 010519/215
Information Exposure	23-04-2019	5	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected and 12.2.0.1 and 18c. Easily exploitable vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS		A-ORA- DATA- 010519/216
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			Base S (Conf. CVSS (CVSS UI:N/	sible dat Score 5.3 identiali Vector: 5:3.0/AV S:U/C:L, D:CVE-	3 ty impa :N/AC:L /I:N/A:N	cts). /PR:N/ V).				
retail_conven	ience_store_b	ack_of	fice							
Improper Access Control	23-04-2019	7.5	Retail Back (Oracle (subce Maint support affecte explore allowe attack access comp Conve Office this ve in una insert some Conve Office as una to a su Conve Office unaut a part (parti Conve	rability Conven Office co e Retail A ompone enance in en	ience St mponer Applicat nt: Leve Function rsion that Easily Ilnerabil Iner	ore nt of ions l 3 ns). The at is lity ed k etail ck cks of result te, s to ck as well access Retail ck and to cause vice e Retail	N/A		A-ORA RETA- 01051	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Typ	pe(s): CSRF- Cross Denial of Service									n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	tch	NCIIF	PC ID
			7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).				
			CVE ID : CVE-2019-2424				
application_te	esting_suite		Walanashilita in the Oreals			T	
Improper Access Control	23-04-2019	6.5	Vulnerability in the Oracle Application Testing Suite component of Oracle Enterprise Manager Products Suite (subcomponent: Load Testing for Web Apps). The supported version that is affected is 13.3.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data as well as unauthorized read access to a subset of Oracle Application Testing Suite accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Testing Suite. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity	N/A		A-ORA APPL- 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
` '	• • •	_	uest Forgery; Dir. Trav Directory Trav oss Site Scripting; Sql- SQL Injection; N 112				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			CVSS (CVSS UI:N/	vailabili Vector: :3.0/AV S:U/C:L, D:CVE-	:N/AC:L /I:L/A:L	/PR:L/).				
retail_point-o	f-service									
Improper Access Control	23-04-2019	7.5	Retail composition of Score Integriting and a composition of the compo	rability Point-o onent of cations ompone tructure ons that 14.0 and itable vu s unauth ter with s via HT romise (of-Servi as of this es to som Point-o sible dat horized set of Or of-Servi and unau y to caus l of servi of Oracl evice. CV 7.3 (Con rity and tts). CVS	f-Service or acle as well as well acle Retail acle Ret	e Retail orted cted are asily lity ed k etail ressful ability rized te cle e l as cess to ail sible d ial cial Pointase ality, lity ::	N/A		A-ORA RETA- 01051	
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 Ty	pe(s): CSRF- Cross Denial of Service								nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			UI:N/	S:U/C:L,	/I:L/A:L).				
			CVE I	D : CVE-	2019-2	558				
jd_edwards_e	nterpriseone	_tools								
Improper Access Control	23-04-2019	4	Edwa Tools JD Ed (subc Runti versic Easily vulne privile netwo comp Enter Succe vulne unaut a subs Enter access Base S (Conf CVSS (CVSS UI:N/	rability rds Enter compore wards P ompone me). The on that is resploit. rability a eged att. ork acces romise J priseOn ssful att rability chorized set of JD priseOn sible dat Score 4.3 identiali Vector: 6:3.0/AV S:U/C:L, D: CVE-	erpriseO ent of Coroducts nt: Web e support s affecte able allows lo acker wit E Tools. acks of t can resu read acc Edward e Tools a. CVSS ty impa :N/AC:L /I:N/A:N	ne Oracle	N/A			A-JD_E- 19/220
Ju_euwarus_w	Voriu_technica	ai_iouii			1 1		I			
Improper Access Control	23-04-2019	5	Edwa Found Oracle (subc Enable version	rability rds Wor dation co e JD Edw ompone ement). ons that A9.3.1 a	ld Tech ompone vards Pr nt: Serv Support are affec	nical nt of oducts ice ted cted are	N/A			A-JD_E- 19/221
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
vuinerability Ty	pe(s): CSRF- Cross Denial of Service	_				_				m; D05-

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
			allow attack access comp World Succe vulne unaut critica access World access (Conf CVSS (CVSS UI:N/	itable vus unauth ser with sovia HT romise Jen Technics all the rability ald the data of the society of the soc	networl TP to D Edwar cal Four acks of t can resu access t r comple D Edwar cal Four ta. CVSS ty impact :N/AC:L /I:N/A:P	rds idation. chis lt in o ete rds idation 3.0 cts).				
configurator										
Improper Access Control	23-04-2019	5	Config Oracle Produ (subc Mode Suppo affect Easily vulne unaut with I HTTP Config attack can re access	erability gurator e Supply acts Suit ompone I Genera orted ve ed are 1 exploit rability chenticat network to comp gurator. as of this esult in u s to criti lete acce	componer Chain e nt: Active ition). rsions the 2.1 and able allows ced attace access veromise Success vulnera inauthor cal data	ent of ve nat are 12.2. ker via Oracle ful ability rized or	N/A		A-ORA CONF- 01051	

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			CVSS (Confi CVSS (CVSS UI:N/	gurator a 3.0 Base identiali Vector: 5:3.0/AV S:U/C:H D: CVE -	Score 7 ty impa :N/AC:L /I:N/A:I	7.5 cts). /PR:N/ N).				
siebel_crm										
Improper Access Control	23-04-2019	6.5	Core-comp CRM (Integral support affects explored allows attack access comp Serve Succes vulne unaut or del Siebel Scripts as unaut to a su Serve access unaut a part (parti Serve 3.0 Ba (Conf.)	rability Server onent of (subcome ration - Serted ver ed is 19. itable vu s high pr ser with s via HT' romise Ser BizLog ssful att rability chorized lete accessi authorized sible dat chorized chorized sible dat chorized	BizLogic Oracle of Oracle of Scripting acks of the Control of Scripting acks of Scripting acks of the Control of Scripting acks of t	c Script Siebel g). The at is dity d k ore - t. chis lit in insert me of izLogic as well access ore - t to cause vice l Core - t. CVSS	N/A			A-SIEB- 19/223
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	pe(s): CSRF- Cross Denial of Service	_				_				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			(CVSS UI:N/	Vector: :3.0/AV S:U/C:L,	/I:L/A:L).				
••			CVE I	D : CVE-	2019-2	570				
soa_suite			77 1	1 :1:	1 0	1	T		T	
Improper Access Control	23-04-2019	5	SOA S Oracle (subce Layer versice 11.1.1 vulne unaut with n HTTP SOA S of this result access SOA S CVSS (Conf. CVSS (CVSS UI:N/	rability uite conce Fusion ompone The sum on that is a sum of the	mponent Middles Int: Fabr Ipported Is affecte Is affect	cof ware ic d d is oitable cker via Oracle attacks an d read Oracle data. 5.3 cts).	N/A		A-ORA SOA 01051	
autovue_3d_p	rofessional_a	dvance	ed							
Information Exposure	23-04-2019	5	AutoV Advar Oracle Produ (subce Handle version	rability Yue 3D P nced con e Supply ncts Suit ompone ling - 2D ons that) and 21	rofession ponent Chain e nt: Forn). Suppo are affect	onal c of nat orted cted are	N/A		A-ORA AUTO 01051	
CV Scoring Scal	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Typ	pe(s): CSRF- Cross Denial of Service	_				-				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	·					tch	NCII	PC ID
			allowal attack access comp 3D Pr Succe vulne unaut a subs 3D Pr access Base S (Confi CVSS (CVSS)	s unauth ter with s via HT' romise (ofession ssful att rability chorized set of Or ofession sible dat Score 5.3 identiali Vector:	Oracle A al Advar acks of t can resu read acc acle Aut al Advar a. CVSS	ed a utoVue nced. his lt in cess to oVue nced 3.0 cts).				
service_bus			CVE I	D : CVE-	2019-2	575				
Improper Access Control	23-04-2019	5	Service Oracle (subce Contain version 11.1.1 12.2.1 vulne unaut with a HTTP Service attack can reability denial DOS)	ce Bus coe Fusion ompone iner). Suons that 1.9.0, 12.13.0. East rability a chenticate to compose Bus. Such of this esult in unit to cause of Oracl	ipported are affed 1.3.0.0 a sily expl	nt of ware I ted are and oitable ker via Oracle all ability rized all aial e Bus.	N/A		A-ORA SERV- 01051	
CV Scoring Scal	e	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	1	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			Vecto (CVSS UI:N/	lability i r: S:3.0/AV S:U/C:N D : CVE -	:N/AC:L /I:N/A:l	/PR:N/ ᠘).				
webcenter_sit	tes									
Improper Access Control	23-04-2019	5	WebCof Ora (subcompleted) of Ora (subcompleted) of Ora (subcompleted) of Ora UI). To that is Easily vulne unaut with INTTP WebCompleted with Interest additional critical access. WebCompleted webCompleted) of CVSS (CVSS UI:N/	rability center Si compone he suppos s affected rexploit rability chenticat hetwork to compone center Si rability cherts conal pro ssful att rability chorized al data o s to all O center Si center Si consider S	tes components on Middent: Advance on Middents of the Advance of t	ponent lleware anced rsion .1.3.0. cker via Oracle le the cle cks act chis lt in o ete core 8.6 cts). /PR:N/ N).	N/A			:- 19/227
Information Exposure	23-04-2019	4	WebC	erability Center Si acle Fusi	tes com	ponent	N/A		A-ORA WEBC 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Access Control 23-04-2019 5.8 Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks require human interaction from a person other than the attacker and	Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
Improper Access Control 23-04-2019 5.8 Supplier_Portal component of Oracle E-Business Suite (subcomponent: Attachments Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks require human interaction from a person other than the attacker and CV Scoring Scale CV Scoring Scale				UI). T that is Easily vulne privil netwo comp WebC attack can re read a Oracle access (Conf CVSS (CVSS UI:N/	he supp s affecte v exploit rability eged att ork acce romise (Center Si as of this esult in u access to e WebCe sible dat Score 4 identiali Vector: S:3.0/AV S:U/C:L	orted ved is 12.2 able allows loacker wiss via HTD racle tes. Success vulnera anauthor a subsector Site a. CVSS 3 ty impacts [N/AC:L/I:N/A:N/A:N/A:N/A:N/A:N/A:N/A:N/A:N/A:N/A	rsion .1.3.0. ow oth TTP to cessful ability rized et of es 3.0 cts).				
Vulnerability in the Oracle iSupplier Portal component of Oracle E-Business Suite (subcomponent: Attachments). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks require human interaction from a person other than the attacker and	isunnlier nor	tal		CVE I	D : CVE-	2019-2	579				
CV Scoring Scale 0.1 1.2 2.3 3.4 4.5 5.6 6.7 7.8 8.0 0.10	Improper Access Control		5.8	iSupp of Ora (subc Attack version 12.1.3 12.2.6 Easily vulne unaut with a HTTP iSupp attack intera	olier Portacle E-Bu ompone hments) ons that 3, 12.2.3 6, 12.2.7 v exploit rability chentical network to comp lier Portacle strequin	tal compusiness Sont: . Supportance affect, 12.2.4, and 12.2.4 able allows teed attack access woromise tal. Success to the compusion a periodical compusion and a periodical compusion	onent Suite eted are 12.2.5, 2.8. eker via Oracle essful n	N/A			
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			Oracle attack impacts Succe vulne unaut critical access Portal as unainsert some Portal 3.0 Ba (Confi Integrity Vecto (CVSS UI:R/S	the vulre is supplied is may so the addition of the control of the	ier Portagnificar onal pro acks of the can result access the carrier is ble dataged update access is is in the carrier is access to a second acts and acts). CV::N/AC:L/AC:L/A:N/AC:L/AC:L/A:N/AC:L/A:N/AC:L/A:N/AC:L/A:N/AC:L/A:N/AC:L/A:N/AC:L/A:N/AC:L/A:N/AC:L/A:N/A	al, atly ducts. chis chis clt in co ete upplier as well cte, s to cier . CVSS				
business_inte	lligence_publ	lisher								
Information Exposure	23-04-2019	4	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks of this			N/A			1-BUSI- 9/230	
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_				_			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). CVE ID: CVE-2019-2588		
Improper Access Control	23-04-2019	5.8	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	N/A	A-ORA-BUSI- 010519/231

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data as well as unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).		
Improper Access Control	23-04-2019	4.9	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher (formerly XML Publisher), attacks may	N/A	A-ORA-BUSI- 010519/232

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data as well as unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/ UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2601		
Improper Access Control	23-04-2019	6.4	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). While the vulnerability is in BI Publisher (formerly XML	N/A	A-ORA-BUSI- 010519/233

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			signification addition addition addition and the vulner unaut or del BI Publis well a access Publis CVSS (Configure 1) (CVSS UI:N/	icantly in onal prossful attrability when here accessions and the stoler (for sher) accessions accession a	oducts. acks of the can result update, ss to son formerly cessible morized baset of Education Education (Education Education E	chis alt in insert me of y XML data as read SI CML data. '.2 'SS				
peoplesoft_en	 terprise_hun	ıan_caj	 pital_m	anagen	nent_tal	lent_acq	uisitior	ı_manaį	ger	
Improper Access Control	23-04-2019								A-ORA PEOP-	
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_	_			_			nformatio	n; DoS-

Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Talent Acquisition Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Talent Acquisition Manager accessible data as well as unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Talent Acquisition Manager accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2590 Dital_management_candidate_gatewa Vulnerability in the PeopleSoft Enterprise HRMS							
peoplesoft_en	terprise_hun	nan_caj	pital_m	anagen	nent_ca	ndidate_	_gatewa	ıy		
Improper Access Control	23-04-2019	5.8	•			N/A		A-ORA PEOP- 01051		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

with network access via HTTP to compromise PeopleSoft Enterprise HRMS. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HRMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HRMS accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HRMS accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U:R/S:C/C:L/I:L/A:N). CVE ID: CVE-2019-2591 email_center Wulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows CV Scoring Scale (CVSS)	Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Par	tch	NCIIPO	: ID
Improper Access Control 23-04-2019 5.8 Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows 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): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-				HTTP to compromise PeopleSoft Enterprise HRMS. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HRMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HRMS accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HRMS accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:L/I:L/A:N).				
Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows CV Scoring Scale (CVSS) O-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-	email_center							
(CVSS) U-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-	Access	23-04-2019	5.8	Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable	N/A		EMAI-	/236
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-	_	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
,		• • •	_				nformation;	DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2600		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows	N/A	A-ORA- EMAI- 010519/237

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2651		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows	N/A	A-ORA- EMAI- 010519/238

0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

CV Scoring Scale

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Pato	ch	NCIII	PC ID
			unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2661				
one-to-one_fu	lfillment						
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E- Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and	N/A		A-ORA - 01051	
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty			uest Forgery; Dir. Trav Directory Trav				
	Denial of Service	; XSS- Cr	oss Site Scripting; Sql- SQL Injection; N 130	I/A- Not App	licable.		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).		
			CVE ID : CVE-2019-2603		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E- Business Suite (subcomponent: Print Server). Supported versions	N/A	A-ORA-ONE- - 010519/240

Vulnerability Type(s)	Publish Date	cvss	Descri	otion & CVE	ID	Pa	tch	NCII	PC ID
Type(s)			that are aff 12.1.2, 12.2.5, 12.2.8. East vulnerability unauthentity with network HTTP to cool One-to-One Successful human interperson oth attacker and vulnerability One-to-One attacks may impact add Successful vulnerability unauthorize	ected are 13, 12.2.3, 2.6, 12.2.7; ly exploita ty allows cated attac ork access empromise e Fulfillmen attacks rec er than the d while th ty is in Ora e Fulfillmen y significan itional pro- attacks of the	2.1.1, 12.2.4, and able cker via Oracle nt. quire om a e acle nt, ntly oducts. chis				
			critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2653						
Improper Access Control	23-04-2019	5.8	Vulnerabili One-to-One component	Fulfillme	nt	N/A		-	A-ONE- 19/241
CV Scoring Scale (CVSS)	e 0-1 pe(s): CSRF- Cross	1-2 Site Reg	2-3 3-4		5-6	6-7 ersal: +In:	7-8 fo- Gain Ir	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Business Suite		
			(subcomponent: Print		
			Server). Supported versions		
			that are affected are 12.1.1,		
			12.1.2, 12.1.3, 12.2.3, 12.2.4,		
			12.2.5, 12.2.6, 12.2.7 and		
			12.2.8. Easily exploitable		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			HTTP to compromise Oracle		
			One-to-One Fulfillment.		
			Successful attacks require		
			human interaction from a		
			person other than the		
			attacker and while the		
			vulnerability is in Oracle		
			One-to-One Fulfillment,		
			attacks may significantly		
			impact additional products.		
			Successful attacks of this		
			vulnerability can result in		
			unauthorized access to		
			critical data or complete		
			access to all Oracle One-to-		
			One Fulfillment accessible		
			data as well as unauthorized		
			update, insert or delete		
			access to some of Oracle		
			One-to-One Fulfillment		
			accessible data. CVSS 3.0		
			Base Score 8.2		
			(Confidentiality and		
			Integrity impacts). CVSS		
			Vector:		
			(CVSS:3.0/AV:N/AC:L/PR:N/		
			UI:R/S:C/C:H/I:L/A:N).		
			CVE ID : CVE-2019-2654		

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

Improper Access 23-04 Control	4-2019		One-to-composite Subcomposite Succession Composite Succession Composite Composite Succession Composite Com	o-One From the one of the	ent: Print orted vers ed are 12 , 12.2.3, 13 , 12.2.7 an exploitab	esions 2.1.1, 2.2.4, and ble eer a Oracle t.				
		4.3	vulner One-te attack impact Succe vulner unaut or del Oracle Fulfill CVSS: (Integ Vector (CVSS UI:R/S	rability in o-One Fixs may sixt additions and attraction action a	while the is in Oracl ulfillment ignificant onal producks of the can result update, in the ses to som	le t, lucts. tin nsert e of data. 7 SS	N/A		A-ORA - 01051	
marketing										
Improper Access 23-04		5.8		•	in the Ora		N/A		A-ORA MARK-	
CV Scoring Scale (CVSS) Vulnerability Type(s): CS	4-2019		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Control			Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2604		010519/243
Improper Access	23-04-2019	5.8	Vulnerability in the Oracle Marketing component of	N/A	A-ORA- MARK-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Control			Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2664		010519/244
Improper Access	23-04-2019	4.3	Vulnerability in the Oracle Marketing component of	N/A	A-ORA- MARK-

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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Control			Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:N/I:L/A:N). CVE ID: CVE-2019-2670		010519/245
Improper Access Control	23-04-2019	4.3	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7	N/A	A-ORA- MARK- 010519/246

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful	N/A	A-ORA- MARK- 010519/247

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			intera other while Oracle may s additi Succe vulne unaut critica access Marke well a insert some access (Confi Integr Vecto (CVSS UI:R/S	:3.0/AV S:C/C:H,	om a pere attacker acting, attacker atty impoducts. acks of the can resurances to access the can resurance access the can resurance access the access to a CVSS 2 ty and acts). CV:L/A:L/A:N/AC:L/I:L/I:L/A:N/AC:L/I:L/A:N/AC:L/I:L/A:N/AC:L/I:L/I:L/A:N/AC:L/I:L/I:L/I:L/I:L/I:L/I:L/I:L/I:L/I:L/I	cson er and y is in acks act chis elt in co ete data as update, s to eting 3.0				
business_inte	lligence		CVEI	D : CVE-	2019-2	0//				
Information Exposure	Vulnerability in the Oracle Business Intelligence Enterprise Edition component of Oracle Fusion Middleware (subcomponent:							1-BUSI- 9/248		
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.									

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			Enter Succe huma perso attack vulne Busin Enter may s additi Succe vulne unaut a subs Intelli Editio 3.0 Ba (Conf CVSS (CVSS /UI:R)	ess Intelleprise Education interaction other resulting interactional processful attrability of the chorized set of Ortigence Education accession accession in accession accessi	ition. acks requestion from the while the is in Oralligence ition, at intly impoducts. acks of the can result read accept	om a e cle tacks act his lt in cess to siness e a. CVSS cts).				
application_o	bject_library	,								
Improper Access Control	23-04-2019	4.3	Application Application Application Comparison (subcontraction Diagnoversical 12.1.3 12.2.6 Easily vulne unaut with 1	Vulnerability in the Oracle Application Object Library component of Oracle E- Business Suite (subcomponent: Diagnostics). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle		N/A		A-ORA APPL- 01051		
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-5						0.0	9-10			

Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSs:3.0/AV:N/AC:L/PR:N/ U!:R/Sc.C/C:N/I:L/A:N). CVE ID : CVE-2019-2621 Service_contracts Vulnerability in the Oracle Service Contracts Component of Oracle E- Business Suite (subcomponent: Renewals). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, A-ORA- Control Improper Access 23-04-2019 4.3 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks require human interaction from a person	Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	atch	NCII	PC ID
Improper Access 23-04-2019 4.3 12.2.6, 12.2.7 and 12.2.8. Control 23-04-2019 4.3 Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks require human interaction from a person				Succe huma perso attack vulne Applicattack impaction or del Orack Library 3.0 Baimpac (CVSS UI:R/	human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).						
Service Contracts component of Oracle E- Business Suite (subcomponent: Renewals). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Control 4.3 Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks require human interaction from a person	service_contr	acts									
CV Scoring Scale	Access	23-04-2019	4.3	Service comp Busin (subce Suppose affect 12.1.3 12.2.6 Easily vulne unaut with the HTTP Service attack	Service Contracts component of Oracle E- Business Suite (subcomponent: Renewals). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks require human		N/A		SERV-		
(CVSC) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9	CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

health_sciences_			while Oracle attack impac Succes vulner unaut or dele Oracle access Base S impac (CVSS	the vulne Service s may sint addition ssful attached horized ete accessible datacters). CVS	e attacke nerability e Contrac ignifican onal proc acks of t can resu update, ss to son e Contrac a. CVSS	y is in cts, tly ducts. his lt in insert ne of cts 3.0				
health_sciences_	, l		01.11		:N/AC:L /I:L/A:N	: /PR:N/				
health_sciences_					2019-2	622				
Improper Access 23 Control	23-04-2019	5.5	Vulnerability in the Oracle Health Sciences Data Management Workbench component of Oracle Health Sciences Applications (subcomponent: User Interface). The supported version that is affected is 2.4.8. Easily exploitable vulnerability allows low				N/A		A-ORA HEAL- 01051	
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)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			unaut a subs Science Work CVSS (Confi Integral Vecto (CVSS UI:N/	sible dat chorized set of Or ces Data bench ac 3.0 Base identiali rity impa r: 5:3.0/AV S:U/C:L,	read acceded Head Manage Score 5 ty and Acts). CV::N/AC:L/A:N	cess to alth ement e data. 6.4 CSS -/PR:L/ -/D).				
work_in_proce	ess									
Improper Access Control	23-04-2019	5.5	Vulnerability in the Oracle Work in Process component of Oracle E-Business Suite (subcomponent: Messages). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Work in Process accessible data as well as unauthorized access to critical data or complete access to all Oracle Work in Process accessible data. CVSS 3.0 Base Score 8.1				N/A		A-ORA WORF 01051	
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 Typ	e(s): CSRF- Cross Denial of Service	_				_			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID: CVE-2019-2633		
general_ledge	er				
Improper Access Control	23-04-2019	5.5	Vulnerability in the Oracle General Ledger component of Oracle E-Business Suite (subcomponent: Consolidation Hierarchy Viewer). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized access to critical data or complete access to all Oracle General Ledger accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/	N/A	A-ORA- GENE- 010519/253

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)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			UI:N/	S:U/C:H	/I:H/A:I	N).				
			CVE I	D : CVE-	2019-2	638				
crm_technica	l_foundation						L			
CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 CV Scoring Scale (CVSS) Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2										-
_	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	pe(s): CSRF- Cross	Site Req	uest For	erv: Dir. 1	rav Dire	ctory Trav	ersal; +In	fo- Gain I	nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2639		
Improper Access Control	23-04-2019	4.3	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector:	N/A	A-ORA- CRM 010519/255

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:N/I:L/A:N). CVE ID : CVE-2019-2669		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2	N/A	A-ORA- CRM 010519/256

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2671		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of	N/A	A-ORA- CRM 010519/257

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2675		
Improper Access Control	23-04-2019	4.3	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data.	N/A	A-ORA- CRM 010519/258

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			(Integ Vector (CVSS UI:R/S		acts). C :N/AC:L /I:L/A:N	VSS ./PR:N/ I).				
trade_manage	ement									
Improper Access Control	23-04-2019	5.8	Trade composition (subcolline) Busin (subcolline) Interference (subcol	., 12.1.2, }, 12.2.5,	ement Oracle ent: User oported are affect 12.1.3, 12.2.6, sily exp allows access veromise ement. acks receivable the sin Oracle than the while the sin Oracle acks of the can result access the can re	cted are 12.2.3, 12.2.7 loitable cker via Oracle quire om a e e cle cttacks act chis alt in co ete cade ole data ed	N/A		A-ORA TRAD 01051	
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_	_			_			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2640		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Trade Management component of Oracle E- Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade	N/A	A-ORA- TRAD- 010519/260

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).		
			Vulnerability in the Oracle Trade Management		
Improper Access Control	23-04-2019	5.8	component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	N/A	A-ORA- TRAD- 010519/261

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Trade Management component of Oracle E- Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact	N/A	A-ORA- TRAD- 010519/262

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:H/I:L/A:N).		
istore			CVE ID : CVE-2019-2643		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle iStore component of Oracle E-Business Suite (subcomponent: Shopping Cart). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle	N/A	A-ORA-ISTO- 010519/263
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Ty		_	uest Forgery; Dir. Trav Directory Trav oss Site Scripting; Sql- SQL Injection; N, 154		

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			signification addition addition addition access access unaut or del Oracle CVSS (Configure 1) (CVSS UI:R/S)	e, attacks icantly it ional pro ssful att rability chorized al data o s to all 0 sible dat chorized ete acce e iStore 3.0 Base identiali rity impa r: S:3.0/AV S:C/C:H, D: CVE-	mpact oducts. acks of the can resurancess to comple a as well update, ss to some accessible Score 8 ty and acts). CV::N/AC:L/I:L/A:N	elt in co ete tore l as insert me of ele data. co exists				
interaction_c	enter_intellig	ence								
Improper Access Control	23-04-2019	5.8	Intera Intelli Oracle (subce Intelli Suppo affecte and 1 vulne unaut with r HTTP Intera Intelli attack intera	erability action Ceargence compone igence (Corted verability action Ceargence Street,	enter compone ness Sui nt: Busi OLTP)). rsions th 2.1.1, 12 sily exp allows ed attac access v oromise enter uccessfu ce huma om a per	nt of te ness nat are 2.1.2 loitable cker via Oracle ul n	N/A		A-ORA INTE- 01051	9/264
CV Scoring Sca (CVSS)	0-1	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Ty	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; Dos- Denial of Service; XSS- Cross Site Scripting; SqI- SQL Injection; N/A- Not Applicable.									

Access Control 23-04-2019 5.8 version that is affected is 11.2.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. 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)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
Commerce_platform Vulnerability in the Oracle Commerce Platform component of Oracle Commerce (subcomponent: Dynamo Application Framework). The supported version that is affected is 11.2.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Interaction Center Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle Interaction Center Intelligence accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).							
Commerce Platform component of Oracle Commerce (subcomponent: Dynamo Application Framework). The supported version that is affected is 11.2.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. CV Scoring Scale (CVSS) O-1 1-2 COMMerce Platform A-ORA-COMM-O10519/265 N/A A-ORA-COMM-O10519/265 N/A COMM-O10519/265	commerce_pl	atform		CVLI	D. CVE	20172	033				
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Improper Access Control	23-04-2019	5.8	Commerce Platform component of Oracle Commerce (subcomponent: Dynamo Application Framework). The supported version that is affected is 11.2.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle			N/A		COMM	I-	
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-	(CVSS)	0-1									

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Platform accessible data as well as unauthorized read access to a subset of Oracle Commerce Platform accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Commerce Platform component of Oracle Commerce (subcomponent: Dynamo Application Framework). Supported versions that are affected are 11.2.0.3 and 11.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform.	N/A	A-ORA- COMM- 010519/266

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			huma perso attack vulne Comm may s additi Succe vulne unaut or del Oracle access unaut a subs Platfo CVSS (Confi Integr Vecto (CVSS	ssful att n intera n other ter and v rability: nerce Pla ignifican onal pro ssful att rability: chorized ete acce e Comm sible dat chorized set of Or rm acce 3.0 Base identiali rity impa r: 6:3.0/AV S:C/C:L/	ction fro than the while the is in Ora atform, a atform, a atform, a atform, a attorm, a to sof t can resu update, ss to sor erce Pla- read acce acle Cora ssible da ty and acts). CV	om a ce cle attacks act chis clt in insert me of tform cess to merce ata. c.1 CSS				
knowledge_m	anagement		CVEI	D: CVE-	2019-2	712				
Improper Access Control	23-04-2019	Vulnerability in the Oracle Knowledge Management component of Oracle E- Business Suite (subcomponent: Setup, Admin). Supported versions that are affected are 12.1.1, N/A						A-ORA KNOW 01051		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2660		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Knowledge component of Oracle Siebel CRM (subcomponent: Web Applications (InfoCenter)). Supported versions that are affected are 8.5.1.0 - 8.5.1.7, 8.6.0 and 8.6.1. Easily exploitable vulnerability allows unauthenticated	N/A	A-ORA- KNOW- 010519/268

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			access comp Know attack intera other while Oracle may s additi Succe vulne unaut or del Oracle data a read a Oracle data. ((Confi Integr Vecto (CVSS UI:R/S	:3.0/AV S:C/C:L/	TP to Dracle uccessfu re huma om a per e attacke nerabilit edge, att ntly imp oducts. acks of t can resu update, ss to sor edge acc s unauth a subse edge acc b Base So ty and acts). CV :N/AC:L /I:L/A:N	of cessible core 6.1				
territory_man	agement									
Improper Access Control	23-04-2019	5.8	Administration). Supported N/A					A-ORA TERR- 01051		
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
vuinerability Typ	pe(s): CSRF- Cross Denial of Service	_	_			-			ntormatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			with r HTTP Territ Succe huma perso attack vulne Territ attack impac Succe vulne unaut critica access Manag as we updat access Territ access Base S (Confi Integr Vector (CVSS UI:R/S	henticate to compare sign attended to compare sign attended to the compare sign attended to some sign attended	access to promise lagement acks requestion from the while the is in Oral agement acks of the can result access the can result access the can result access the can result accessible or delevation and the can result accessible access	Oracle of. quire om a e cle of, otly ducts. chis clt in co ete erritory ole data ed te cle of,				
advanced_out	bound telen	hony	CVLI	D. CVL	20172	002				
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Advanced Outbound Telephony component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are				N/A		A-ORA ADVA 01051	
CV Scoring Scale (CVSS)	e 0-1 pe(s): CSRF- Cross	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
vuinerability Typ	Denial of Service	_	_			-				11, 003-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12.1.1, 12.1.2, 12.1.3, 12.2.3,		
			12.2.4, 12.2.5, 12.2.6, 12.2.7		
			and 12.2.8. Easily exploitable		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			HTTP to compromise Oracle		
			Advanced Outbound		
			Telephony. Successful		
			attacks require human		
			interaction from a person		
			other than the attacker and		
			while the vulnerability is in		
			Oracle Advanced Outbound		
			Telephony, attacks may		
			significantly impact		
			additional products.		
			Successful attacks of this		
			vulnerability can result in		
			unauthorized access to		
			critical data or complete		
			access to all Oracle		
			Advanced Outbound		
			Telephony accessible data as		
			well as unauthorized update,		
			insert or delete access to		
			some of Oracle Advanced		
			Outbound Telephony		
			accessible data. CVSS 3.0		
			Base Score 8.2		
			(Confidentiality and		
			Integrity impacts). CVSS		
			Vector:		
			(CVSS:3.0/AV:N/AC:L/PR:N/		
			UI:R/S:C/C:H/I:L/A:N).		
			CVE ID : CVE-2019-2663		
common_app	lications				

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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PCID
Improper Access Control	23-04-2019	5.8	Comp Busin (subc Mana Suppo affect 12.2.4 and 1 vulne unaut with n HTTP Comn Succe huma perso attack vulne Comn attack impac Succe vulne unaut critica access Applica as we updat access (Conf Integr Vecto	non Apponent of ess Suite ompone gement orted vere dare 1 4, 12.2.5, 2.2.8. Earability and the twork to component and the rability and Apposs may set additions and the rability and the storage of the s	nt: CRM Framew rsions the 2.1.3, 12 12.2.6, sily expladlows ted attace access were comise dications acks requestion from than the while the dis in Ora dications acks of the can resu access the racle Complete accessible uthorize or delete e of Orac dications a. CVSS	User ork). lat are l.2.3, loitable ker ria Oracle s. uire om a cle chis lt in o ete mmon e data ed ce cle s, 3.0	N/A		A-ORA COMM 01051	-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			UI:R/	S:C/C:H	/I:L/A:N	í).				
			CVE I	D : CVE-	2019-2	665				
applications_	framework									
Improper Access Control	23-04-2019	5.8	Application of del Oracle Frame	cations less Suite ompone of the design and the composition of the composition of the cations less may set additions less may set additio	Framew Foracle Int: File Up rsions th 2.1.3, 12 12.2.6, sily exp allows red attace access veromise Framew acks requestion fro than the while the is in Ora Framew acks of t can resu access t r comple racle Framew a as wel update, ss to son ations ccessible	ork E- oload). nat are 2.2.3, 12.2.7 loitable cker via Oracle ork. quire om a e cle ork, ntly ducts. chis clt in co ete ork l as insert me of	N/A		A-ORA APPL- 01051	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	()	011 0								

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID					itch	NCII	PC ID
			Integrated Vector (CVSS UI:R/S	identiali rity impa r: 5:3.0/AV S:C/C:H, D: CVE -	acts). CV :N/AC:L /I:L/A:N	./PR:N/ I).				
mysql_connec	ctor/j									
Improper Input Validation	23-04-2019	3.5	Conne Oracle (subce Conne versice 8.0.15 explosi high p logon where execu MySQ Succe huma perso attack of this result Conne Score Integri impac (CVSS UI:R/S	rability ectors co e MySQL ompone ector/J). ons that ons that on other orivilege to the in e MySQL tes to co L Conne ssful att n intera n other orivilege in takeo ectors. Co 6.3 (Con rity and cts). CVS S:U/C:H D: CVE-	omponer ont: Suppor are affect or. Difficability a d attack offrastruct connect omprom ectors. acks requestion from than the ability can be a	ted cted are cult to allows ter with cture ctors ise muire om a ettacks an MySQL Base ality, lity c: //PR:H/ H).	N/A		A-ORA MYSQ 01051	
peoplesoft_en	iterprise_elm			gement						
Improper Access	23-04-2019	Vulnerability in the PeopleSoft Enterprise ELM component of Oracle A-ORA- PEOP-								
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_				_				on; DoS-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIII	PCID
Control			PeopleSoft Products (subcomponent: Enterprise Learning Mgmt). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise ELM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSo Enterprise ELM accessible data. CVSS 3.0 Base Score 4 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L UI:N/S:U/C:N/I:L/A:N). CVE ID: CVE-2019-2700	01051	9/274		
hospitality_cr	uise_dining_r	oom_n	Vulnerability in the Oracle				
Improper Input Validation	23-04-2019	6.4	Hospitality Cruise Dining Room Management component of Oracle Hospitality Applications (subcomponent: Web Service). The supported version that is affected is 8.0.80. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracl Hospitality Cruise Dining Room Management. While	N/A e		A-ORA HOSP- 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
	• • • •	_	uest Forgery; Dir. Trav Directory T oss Site Scripting; Sql- SQL Injection			nformatio	n; DoS-

Access Control 23-04-2019 5.8 BPM Foundation Services). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via 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)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
A-ORA-BUSI-Ontrol 23-04-2019 5.8 Supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via CV Scoring Scale (CVSS) O-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 9-10 1-2				Hospi Room may s additi Success vulner unaut critica access Hospi Room access unaut or del Oracle Dining access (Confi Integr Vector (CVSS UI:N/S	tality Cr Manage ignificant onal prossful attrability horized al data of sto all Ottality Cr Manage sible date horized ete acce et Hospit g Room sible date Score 9.3 identiality imparts: :3.0/AV S:C/C:H	ement, antly impoducts. acks of the can result access the can result access the can result and as well and acts to some ality Crumanage and CVSS and acts). CV: L'I:L/A:N	ttacks act chis alt in co ete ning ll as insert me of uise ment 3.0 CSS A/PR:N/ I).				
Business Process Management Suite component of Oracle Fusion Middleware (subcomponent: BPM Foundation Services). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	business_prod	cess_manager	nent_s								
(CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Improper Access Control	23-04-2019	5.8	Busing Manage composition Middl BPM I The suits affe Easily vulner unaut	ess Processes Pr	sess Suite Foracle subcompion Served version 1.1.1.9.0 able allows	Fusion ponent: rices). n that 0.	N/A			
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-	(CVSS)	0-1									

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			Busin Manage Succe huma perso attack vulne Busin Manage additi Succe vulne unaut critica access Proce access unaut or del Oracle Manage access (Confi Integri Vecto (CVSS UI:R/S	5:3.0/AV S:C/C:H _/ D : CVE -	sess Suite. acks requestion from the than the while the sis in Oracess Suite, at acks of the can result access to some six access the can result access the can result access to some six access to some six access. CVSS 2 ty and access. CVSS 2 ty access.	quire om a e ccle tacks act chis clt in co ete usiness Suite l as insert me of ess 3.0				
peoplesoft_en	iterprise_lear	ning_n	ıanage	ment						
Improper Access Control	23-04-2019	5.8	Enterprise Learning N/A PEOI						A-ORA PEOP- 01051	
CV Scoring Scal (CVSS) Vulnerability Ty	e 0-1 pe(s): CSRF- Cross Denial of Service	_							8-9 nformatio	9-10 on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Search). The supported		
			version that is affected is 9.2.		
			Easily exploitable		
			vulnerability allows		
			unauthenticated attacker		
			with network access via		
			HTTP to compromise		
			PeopleSoft Enterprise ELM		
			Enterprise Learning		
			Management. Successful		
			attacks require human		
			interaction from a person		
			other than the attacker and		
			while the vulnerability is in		
			PeopleSoft Enterprise ELM		
			Enterprise Learning		
			Management, attacks may		
			significantly impact		
			additional products.		
			Successful attacks of this		
			vulnerability can result in		
			unauthorized update, insert		
			or delete access to some of		
			PeopleSoft Enterprise ELM		
			Enterprise Learning		
			Management accessible data		
			as well as unauthorized read		
			access to a subset of		
			PeopleSoft Enterprise ELM		
			Enterprise Learning		
			Management accessible data.		
			CVSS 3.0 Base Score 6.1		
			(Confidentiality and		
			Integrity impacts). CVSS		
			Vector:		
			(CVSS:3.0/AV:N/AC:L/PR:N/		
			UI:R/S:C/C:L/I:L/A:N).		
			CVE ID : CVE-2019-2707		

 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)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIIF	PC ID
commerce_m	erchandising									
Improper Access Control	23-04-2019	6.4	Comp Comp Comp Asset support affect explorations access comp Comp Succes vulned unau or de Oracl Merce data a read Oracl Merce data a (Conf Integ Vector (CVS)	erability merce Monent of merce (see Manage orted vected is 11 oitable vected is 11 ortable v	erchand f Oracle ubcomporer). The rsion that 2.0.3. Ea ulnerabil nenticate networl TP to Oracle erchand acks of t can resu update, ess to son erce ag access s unauth o a subse erce ag access s unauth o a subse erce d access UBase So ity and acts). CV	onent: at is asily lity ed k ising. chis alt in insert me of sible core 6.5 SS JPR:N/ I).	N/A		A-ORA COMM 01051	-
Information Exposure	23-04-2019	3.5	Vulnerability in the Oracle Data Integrator component of Oracle Fusion Middleware (subcomponent: ODI Tools). Supported versions that are				N/A		A-ORA DATA- 01051	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

(CVSS)

Vulnerability Type(s)	Publish Date	cvss	1	Description	Description & CVE ID		Pa	itch	NCII	PC ID
			affected are 11.1.1.9.0 and 12.2.1.3.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Data Integrator. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Data Integrator accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).							
weblogic_serv	von		CVE I	D : CVE-	2019-2	720				
Improper Access Control	23-04-2019	4	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in			N/A		A-ORA WEBL 01051		
CV Scoring Scal										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N). CVE ID: CVE-2019-2568		
Information Exposure	23-04-2019	4	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:U/C:H/I:N/A:N). CVE ID: CVE-2019-2615	N/A	A-ORA- WEBL- 010519/281
Improper Access Control	23-04-2019	5.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core	N/A	A-ORA- WEBL- 010519/282

 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)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U:N/S:U/C:H/I:L/A:N).		
Improper Access Control	23-04-2019	7.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful	N/A	A-ORA- WEBL- 010519/283

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). CVE ID: CVE-2019-2645		
Improper Access Control	23-04-2019	7.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: EJB Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:N/S:U/C:H/I:H/A:H). CVE ID: CVE-2019-2646	N/A	A-ORA- WEBL- 010519/284
Information Exposure	23-04-2019	5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web	N/A	A-ORA- WEBL- 010519/285

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).		
Information Exposure	23-04-2019	5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible	N/A	A-ORA- WEBL- 010519/286

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). CVE ID: CVE-2019-2648		
Information Exposure	23-04-2019	5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/ UI:N/S:U/C:H/I:N/A:N).	N/A	A-ORA- WEBL- 010519/287
			CVE ID : CVE-2019-2649		
Information Exposure	23-04-2019 5 (subcomponent: WI S - Woh		N/A	A-ORA- WEBL- 010519/288	

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).		
			CVE ID : CVE-2019-2650		
Improper Access Control	23-04-2019	7.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/	N/A	A-ORA- WEBL- 010519/289

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
			ĺ	S:U/C:H D : CVE-	•					
e-business_su	iite									
Improper Access Control	23-04-2019	5.8	One-t comp Busin (subconserved that a 12.1.2 for 12.2.5	rability o-One From the component of the	alfillment oracle of the acks required than the acks of the acks o	ersions 2.1.1, 12.2.4, and ble cker via Oracle nt. quire om a cle cle nt, ntly ducts. chis clt in co ete ne-to- sible norized te cle nt	N/A		A-ORA BU- 01053	A-E- 19/290
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
vunierability Ty	pe(s): CSRF- Cross Denial of Service								mormatic	ni, DU3-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID: CVE-2019-2551		
peoplesoft_er	nterprise_peo	pletool	s		
Improper Access Control	23-04-2019	4.3	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Fluid Homepage & Navigation). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). CVE ID: CVE-2019-2573	N/A	A-ORA- PEOP- 010519/291

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	23-04-2019	4	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: RemoteCall). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/ UI:N/S:U/C:L/I:N/A:N). CVE ID: CVE-2019-2586	N/A	A-ORA- PEOP- 010519/292
Improper Access Control	23-04-2019	4.9	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: Application Server). Supported versions that are affected are 8.55, 8.56 and 8.57. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft	N/A	A-ORA- PEOP- 010519/293

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID: CVE-2019-2594		
Improper Access Control	23-04-2019	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks	N/A	A-ORA- PEOP- 010519/294

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)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).		
Improper Access Control	23-04-2019	5.5	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: SQR). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation,	N/A	A-ORA- PEOP- 010519/295

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)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/ UI:N/S:C/C:H/I:H/A:N). CVE ID: CVE-2019-2598		
Improper Access Control	23-04-2019	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products.	N/A	A-ORA- PEOP- 010519/296

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

database Improper Access Control 23-04-	proper cess 23-04-2019 4		vulner unaut or del People as wel access People CVSS 3 (Confi Integr Vector (CVSS	rability of horized ete accesses of English as unared to a subsection of the English and the English and Base dentiality impared to 13.0/AV:	ccessible uthorized oset of terprise ccessible Score 6.1 ty and acts). CVS	data data.				
Improper Access 23-04-			CVE II		:N/AC:L/ 'I:L/A:N). 2019-26	,				
Access 23-04										
	4-2019	4.6	Cluster Oracle Support affecter 12.1.0 Easily vulner privile Grid In privile infrast Portal execut Portal the vu Portal attack impac	erware contents of the Databa ported versed are 11 and 12. And	0.1 and 1 able allows hig acker hav cture Use logon to where erware mpromis terware. V	at of c. at are 8c. gh ing er the While	N/A		A-ORA DATA- 01051	
CV Scoring Scale (CVSS)		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

vulnerability can result in takeover of Portable Clusterware. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/U:N/S:C/C:H/I:H/A:H). CVE ID : CVE-2019-2619 Osticket Osticket Osticket In osTicket before 1.12, XSS exists via /upload/scp/lusers, sph?do=import-users, and /upload/scp/lusers, sph?do=import-users, and /upload/scp/ajax.php/users /import if an agent manager user uploads a crafted .csv file to the User Importer, because file contents can appear in an error message. The XSS can lead to local file inclusion. CVE ID : CVE-2019-11537 PHP Php When processing certain files, PHP EXIF extension in versions 7.1.x below 7.2.1 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in exif_process_IPD_TAG function. This may lead to information disclosure or crash. CVS coring Scale (CVS)	Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
Improper Neutralizatio no finput During Web Page Generation ('Cross-site Scripting') PHP php Improper Restriction of Operations O				takeo Cluste Score Integr impac (CVSS UI:N/	ver of Poerware. (8.2 (Coority and ets). CVS:3.0/AVS:C/C:H	ortable CVSS 3.0 ofidentia Availabi S Vector :L/AC:L /I:H/A:F	Base ality, lity :: /PR:H/ I).				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') Improper Restriction of Operations within the Bounds of a Memory Buffer Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') Improper Restriction of Operations within the Bounds of a Memory Buffer Improper N/A In osTicket before 1.12, XSS exists via /upload/file.php, //upload/scp/users.php?do=i mport-users, and //upload/scp/users.php/users //A -OST-OSTI- 010519/298	Osticket										
exists via /upload/file.php, /upload/scp/users.php?do=i mport-users, and /upload/scp/ajax.php/users /import if an agent manager user uploads a crafted .csv file to the User Importer, because file contents can appear in an error message. The XSS can lead to local file inclusion. CVE ID: CVE-2019-11537 PHP Php When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash.	osticket										
Php Improper Restriction of Operations within the Bounds of a Memory Buffer CV Scoring Scale CV Scoring Scale	Neutralizatio n of Input During Web Page Generation ('Cross-site	25-04-2019	4.3	exists /uplo mpor /uplo /impo user u file to becau appea The X inclus	via /up ad/scp/ t-users, ad/scp/ ort if an uploads the Use use file cour in an e SS can lesion.	load/file users.ph and ajax.php agent m a crafted r Impor ontents error me ead to lo	e.php, np?do=i o/users anager l.csv ter, can essage. cal file	N/A			
When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash. CV Scoring Scale Out 1.2 2.3 3.4 4.5 5.6 6.7 7.8 8-9 9-10	PHP										
Improper Restriction of Operations within the Bounds of a Memory Buffer CV Scoring Scale Of Restriction of Operations of Operations within the Bounds of a Memory Buffer Improper files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash. CV Scoring Scale Out 1.2 2.3 3.4 4.5 5.6 6.7 7.8 8.9 9.10	php										
- 1-1 1-1 1-1 1-1 1-1 1-1 1-1 1-1 1-1 1	Restriction of Operations within the Bounds of a Memory	18-04-2019	6.4	files, l versic 7.2.x l below read p exif_p functi inform	PHP EXIons 7.1.x below 7. 7.3.4 capast allo process_land. This mation d	F extens below 7 2.17 and an be can cated bu FD_TAG may lea	ion in 7.1.28, d 7.3.x used to affer in	N/A			
	_	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11034		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-04-2019	6.4	When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in exif_iif_add_value function. This may lead to information disclosure or crash.	N/A	A-PHP-PHP- 010519/300
			CVE ID : CVE-2019-11035		
Pluck-cms					
pluck					
Unrestricted Upload of File with Dangerous Type	19-04-2019	7.5	data/inc/files.php in Pluck 4.7.8 allows remote attackers to execute arbitrary code by uploading a .htaccess file that specifies SetHandler x-httpd-php for a .txt file, because only certain PHP-related filename extensions are blocked. CVE ID: CVE-2019-11344	N/A	A-PLU- PLUC- 010519/301
Projectsend					
projectsend					
Unrestricted Upload of File with Dangerous Type	20-04-2019	6.5	An issue was discovered in ProjectSend r1053. upload-process-form.php allows finished_files[]=/ directory traversal. It is possible for users to read arbitrary files and (potentially) access the supporting database, delete arbitrary files, access user passwords, or run arbitrary	N/A	A-PRO- PROJ- 010519/302

CV Scoring Scale	0_1	1_2	2-3	3-/1	<i>1</i> -5	5-6	6-7	7-8	8 _0	9-10
(CVSS)	0-1	1-2	2-3	3-4	4-5	3-0	0-7	7-8	0-3	3-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			code. CVE ID : CVE-2019-11378		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	26-04-2019	4.3	Cross-site scripting (XSS) vulnerability in ProjectSend before r1070 allows remote attackers to inject arbitrary web script or HTML. CVE ID: CVE-2019-11533	https://www .projectsend. org/change- log/	A-PRO- PROJ- 010519/303
Qemu					
qemu					
NULL Pointer Dereference	19-04-2019	5	hw/sparc64/sun4u.c in QEMU 3.1.50 is vulnerable to a NULL pointer dereference, which allows the attacker to cause a denial of service via a device driver. CVE ID: CVE-2019-5008	N/A	A-QEM- QEMU- 010519/304
Redhat					
keycloak					
Information Exposure	24-04-2019	5.5	Keycloak up to version 6.0.0 allows the end user token (access or id token JWT) to be used as the session cookie for browser sessions for OIDC. As a result an attacker with access to service provider backend could hijack user?s browser session. CVE ID: CVE-2019-3868	https://bugzi lla.redhat.co m/show_bug. cgi?id=CVE- 2019-3868	A-RED- KEYC- 010519/305
rocboss					
rocboss					

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)	CSRF_ Cro	se Sita Ra	auest For	gery: Dir 1	Tray - Dire	ctory Tray	orsal• ±In	fo- Gain Ir	formation	n· DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-04-2019	7.5	ostCo ROCB inject Post:c paran by the	controller. OSS V2 ion via t doRewar nter, as c e /do/re D: CVE-	php in 2.1 has S he d score lemonst ward/3	SQL crated URI.	N/A		A-RO0 ROCB 01051	
Sem-cms										
Semcms										
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	25-04-2019	6.5	SEMC SEMC AID[] the cla inject mechan	sue was of MS 3.8. MS_Inque SQL Inject ass.phprect check_sanism is the control of	niry.php ection be nailer.pl eql prote incomp	allows ecause hp ection lete.	N/A		A-SEM SEMC 01051	
Siemens										
simatic_cp44	3-1_opc_ua									
Improper Input Validation	17-04-2019	5	identi versic (All ve CP343 versic (All versic OPC U SIMA7 (All versic	nerabilit fied in Cons), CP1 ons), SIA ersions), 3-1 Adva ons), SIM ersions), JA (All v TIC ET 2 oller CP ersions «	P1604 (All 616 (All MTIC RI) SIMATION (ALL ATIC CINT) Anced (ALL ATIC CINT) ANCED (ALL ATIC CINT) OO SP OO (U 1515) V2.1.6	(All ll F185C IC Ill P443-1 IC Ill P443-1 I, pen SP PC	N/A			-SIMA- 19/308
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_							nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIII	PC ID
			Controller CPU 1515SP PC2				
			(All versions), SIMATIC HM				
			Comfort Outdoor Panels 7"	&			
			15" (All versions), SIMATIC				
			HMI Comfort Panels 4" - 22'	ort Panels 4" - 22" ns), SIMATIC HMI e Panels KTP400F, TP700F, KTP900 OOF (All versions), PC DiagMonitor ns), SIMATIC (All versions), F182C (All SIMATIC RF186C ns), SIMATIC ll versions), F600R (All SIMATIC S7-1500 (All versions), 7-1500 Software (All versions), 7-300 CPU family ns < V3.X.16), 7-400 PN (incl. F) ow (All versions), 7-400 PN/DP V7 ll versions), 7-PLCSIM (All versions), eleservice Advanced (All SIMATIC e Adapter IE Basic ns), SIMATIC			
			(All versions), SIMATIC HM				
			KTP Mobile Panels KTP4001	F,			
			KTP700, KTP700F, KTP900				
			und KTP900F (All versions)	,			
			SIMATIC IPC DiagMonitor				
			(All versions), SIMATIC				
			RF181-EIP (All versions),				
			SIMATIC RF182C (All				
			versions), SIMATIC RF186C				
			(All versions), SIMATIC				
			RF188C (All versions),				
			SIMATIC RF600R (All				
			versions), SIMATIC S7-1500)			
			CPU family (All versions),				
			SIMATIC S7-1500 Software				
			Controller (All versions),				
			SIMATIC S7-300 CPU family	,			
			(All versions $<$ V3.X.16),				
			SIMATIC S7-400 PN (incl. F)	1			
			` '				
			` ,	,			
			•				
			(incl. F) (All versions),				
			SIMATIC S7-PLCSIM				
			Advanced (All versions),				
			SIMATIC Teleservice				
			Adapter IE Advanced (All				
			versions), SIMATIC				
			Teleservice Adapter IE Basi	С			
			(All versions), SIMATIC				
			Teleservice Adapter IE				
			Standard (All versions),				
		SIMATIC WinAC RTX 2010					
			(All versions), SIMATIC				
			WinCC Runtime Advanced				
CV Scoring Sca	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)	0-1	1-2	2 3 3-4 4-5 5-0	0-7	7-0	0-3	5-10

Vulnerability Type(s)	(All versions), SIMOCODE pro V EIP (All versions), SIMOCODE pro V PN (All versions), SIMOCODE pro V PN (All versions), SINAMICS G130 V4.6 (All versions), SINAMICS G130 V4.7 (All versions), SINAMICS G130 V4.7 (All versions), SINAMICS G130 V4.8 (All versions), SINAMICS G130 V5.1 (All versions), SINAMICS G130 V5.1 (All versions), SINAMICS G150 V5.1 (All versions), SINAMICS G150 V4.6 (All versions), SINAMICS G150 V4.6 (All versions), SINAMICS G150 V4.7 (All versions), SINAMICS G150 V4.7 (All versions versions), SINAMICS G150 V5.1 (All vers	NCIII	PC ID						
			(All vers	ions), SIMOC	ODE				
			pro V EI	P (All version	s),				
			SIMOCO	DE pro V PN ([All				
			versions), SINAMICS (G130				
			V4.6 (Al	l versions),					
			SINAMIO	CS G130 V4.7	(All				
			versions), SINAMICS (G130				
			V4.7 SP1	(All versions	s),				
			SINAMIO	CS G130 V4.8	(All				
			versions	< V4.8 HF6),					
			SINAMIO	CS G130 V5.1	(All				
			versions), SINAMICS (G130				
			V5.1 SP1	(All versions	s < V5.1				
				•					
			`	-	(All				
					`				
				•					
				•	-				
					`				
				-					
					`				
				•					
				-	7120				
					(Δ11				
					`				
				•					
				•	-				
					(AII				
				-	(A 11				
					`				
				•					
				•	5150				
	SINAMICS S150 V4.7 (All								
					-				
				•					
				•	-				
			SINAMIO	LS S150 V4.8	(All				
CV Scoring Sca	le 0-1	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty									

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PCID
			versio	ns < V4	.8 HF6),					
			SINA	AICS S15	50 V5.1	(All				
			versio	ns), SIN	AMICS S	5150				
			V5.1 S	SP1 (All	versions	s < V5.1				
			SP1 H	F4), SIN	AMICS S	5210				
			V5.1 (All vers	ions),					
			SINA	AICS S2						
			(All v							
			Mana	ger (All	versions	s),				
			SITOF	PSU86	00 (All					
			versio	ns), SIT	OP UPS:	1600				
			(All v	ersions)						
			(All v	ersions)	. The					
			webse	erver of						
			devic	es conta	ins a					
			vulne	rability	that may	lead				
			to a d	enial-of-	service					
			condi	tion. An	attackei	may				
			cause	a denia	-of-serv	ice				
			situat	ion whic	ch leads	to a				
			restar	t of the	webserv	er of				
			the af	fected d	evice. Tł	ne				
			secur	ity vulne	rability	could				
			be exp	oloited b	y an att	acker				
			with 1	network	access t	o the				
			affect	ed syste	ms. Succ	essful				
			explo	itation r	equires	no				
			syster	n privile	ges and	no				
			-	nteracti	_					
			could	use the	vulnera	bility				
						bility of				
				vice. At		-				
			adviso	ory publ	ication 1	10				
				exploit						
			_	ity vulne						
			know	-	- 5					
				D : CVE-	2019-6	568				
simatic_ipc_di	iagmonitor									
CV Scoring Scal	e									
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

		CVSS	Description & CVE ID	Pate		NCIIP	
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF188 (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443 (All versions), SIMATIC CP443-1 Advanced (All versions), SIMATIC CP443 (All versions), SIMATIC CP443 (All versions), SIMATIC CP443 (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions), SIMATIC HCOMFORT Outdoor Panels 37 (All versions), SIMATIC HCOMFORT Panels 4" - 27 (All versions), SIMATIC HCOMFORT Panels KTP40 (KTP700, KTP700F, KTP90 und KTP900F (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF188C (All versions), SIMATIC S7-1500 Softwar Controller (All versions), SIMATIC S7-300 CPU family (All versions), SIMATIC S7-400 PN (incl. SIMATIC S7	35C 33-1 33-1 a PC a PC2 HMI 7" & FIC 22" HMI -00F, 000 ons), or), 36C 500), are , nily		A-SIE-S 010519	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5	5-6 6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description &	CVE ID	Pat	ch	NCIII	PC ID
			V6 and below (All	versions),				
			SIMATIC S7-400 F	N/DP V7				
			(incl. F) (All version	ons),				
			SIMATIC S7-PLCS	M				
			Advanced (All ver	sions),				
			SIMATIC Teleserv	ice				
			Adapter IE Advan	ced (All				
			versions), SIMATI					
			Teleservice Adapt	er IE Basic				
			(All versions), SIM	ATIC				
			Teleservice Adapt	er IE				
			Standard (All vers	ions),				
			SIMATIC WinAC R					
			(All versions), SIM					
			WinCC Runtime A					
			(All versions), SIM					
			pro V EIP (All vers					
			SIMOCODE pro V	-				
			versions), SINAMI	•				
			V4.6 (All versions)					
			SINAMICS G130 V					
			versions), SINAMI					
			V4.7 SP1 (All vers					
			SINAMICS G130 V	-				
			versions < V4.8 Hl					
				,				
			SINAMICS G130 V	•				
			versions), SINAMI					
			V5.1 SP1 (All vers					
			SP1 HF4), SINAMI					
			V4.6 (All versions)					
			SINAMICS G150 V					
			versions), SINAMI					
			V4.7 SP1 (All vers					
			SINAMICS G150 V	•				
			versions < V4.8 HI	•				
			SINAMICS G150 V	-				
			versions), SINAMI	CS G150				
			V5.1 SP1 (All vers	ions < V5.1				
			SP1 HF4), SINAMI	CS S120				
CV Scoring Sca	e 0-1	1-2	2-3 3-4 4-	5 5-6	6-7	7-8	8-9	9-10
(CVSS)	0-1	1-2	3-4 4-	3-0	0-7	7-0	0-3	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pate	ch	NCIII	PC ID
			V4.6 (All versions),				
			SINAMICS S120 V4.7 (All				
			versions), SINAMICS S120				
			V4.7 SP1 (All versions),				
			SINAMICS S120 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S120 V5.1 (All				
			versions), SINAMICS S120				
			V5.1 SP1 (All versions < V	5.1			
			SP1 HF4), SINAMICS S150				
			V4.6 (All versions),				
			SINAMICS S150 V4.7 (All				
			versions), SINAMICS S150				
			V4.7 SP1 (All versions),				
			SINAMICS S150 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S150 V5.1 (All				
			versions), SINAMICS S150				
			V5.1 SP1 (All versions < V	5.1			
			SP1 HF4), SINAMICS S210				
			V5.1 (All versions),				
			SINAMICS S210 V5.1 SP1				
			(All versions), SITOP				
			Manager (All versions),				
			SITOP PSU8600 (All				
			versions), SITOP UPS1600				
			(All versions), TIM 1531 I				
			(All versions). The				
			webserver of the affected				
			devices contains a				
			vulnerability that may lead	d			
			to a denial-of-service				
			condition. An attacker may	.,			
			cause a denial-of-service				
			situation which leads to a				
			restart of the webserver o	f			
			the affected device. The	•			
			security vulnerability coul	d			
			be exploited by an attacke				
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-	6 6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross		3 13 3				

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
	matic_s7-1500_software_cont				access to ms. Success and con. An access and con. An access and con. An access	cessful no no ttacker bility bility of e of no this				
simatic e7-15	00 coftware	contro		D : CVE-	2019-6	568				
Jimutic_3/-1J	Jog Joitwai C	conti o	1	nerabilit	y has be	en				
Improper Input 17-04-2019 5		versice (All versi	fied in Cons), CP1 cons), SIA crsions), 3-1 Adva cons), SIM crsions), 3-1 Adva cons), SIM crsions), GA (All versions of CP1 crsions of CP1 crsions), crt Outd All versions Comfort crsions) Mobile Pa COO, KTP2 TTP900F	MTIC RI MTIC RI MTIC RI Anced (A IATIC CI INTIC CI INTIC INTIC CI INTIC CI INTIC CI INTIC CI INTIC CI INTIC CI INTIC CI	F185C F185C IC III P443-1 IC III P443-1 , pen FP PC IC HMI els 7" & MATIC " - 22" IC HMI FP400F, FP900	N/A			SIMA- .9/310	
CV Scoring Scal							6-7	7-8		

Vulnerability Type(s)	Publish Date	cvss	Descr	iption & CVE	ID	Pa	tch	NCIII	PC ID
			SIMATIC I	PC DiagMor	itor				
			(All versio	ns), SIMAT	C				
			RF181-EIF	(All versio	ns),				
			SIMATIC R	F182C (All	-				
			versions),	SIMATIC RI	F186C				
			(All versio	ns), SIMAT					
			RF188C (A	ll versions)	,				
			SIMATIC R	F600R (All					
			versions),	SIMATIC S7					
			CPU family	(All versio	ns),				
			SIMATIC S	7-1500 Sof					
			Controller	(All version	ıs),				
			SIMATIC S	7-300 CPU	family				
			(All versio	ns < V3.X.1	6),				
			`	7-400 PN (i	-				
			V6 and bel	ow (All ver	sions),				
				7-400 PN/I					
				ll versions)					
			SIMATIC S	_					
			Advanced	(All version	ıs),				
			SIMATIC T	-	<i>y.</i>				
			Adapter IE	Advanced	(All				
			versions),						
			-	e Adapter II	E Basic				
				ns), SIMATI					
			`	e Adapter II					
				All versions					
			`	VinAC RTX	-				
				ns), SIMAT					
			-	ntime Adva					
				ns), SIMOC					
			`	All version					
			-	E pro V PN (-				
				SINAMICS (•				
			Versions), V4.6 (All v		1100				
			`	G130 V4.7	(All				
				SINAMICS (`				
				All versions					
			SINAMICS						
CV Scoring Sca	le 0-1	1-2	2-3 3-4	1 4-5	5-6	6-7	7-8	8-9	9-1
(CVSS)	<u> </u>				3 0	J ,	, ,	5 5	1

Vulnerability Type(s)	Publish Date	cvss	Description & CVE	ID Pa	tch	NCIII	PC ID
			versions < V4.8 HF6),				
			SINAMICS G130 V5.1	(All			
			versions), SINAMICS	G130			
			V5.1 SP1 (All versions	s < V5.1			
			SP1 HF4), SINAMICS	G150			
			V4.6 (All versions),				
			SINAMICS G150 V4.7	(All			
			versions), SINAMICS	-			
			V4.7 SP1 (All versions				
			SINAMICS G150 V4.8				
			versions < V4.8 HF6),	`			
			SINAMICS G150 V5.1				
			versions), SINAMICS	•			
			V5.1 SP1 (All versions				
			SP1 HF4), SINAMICS				
			V4.6 (All versions),	7120			
			SINAMICS S120 V4.7	CAII			
			versions), SINAMICS	`			
			V4.7 SP1 (All versions				
			SINAMICS S120 V4.8				
			versions < V4.8 HF6),	`			
			SINAMICS S120 V5.1				
			versions), SINAMICS	`			
			V5.1 SP1 (All versions				
			•				
			SP1 HF4), SINAMICS	5150			
			V4.6 (All versions),	C A 11			
			SINAMICS S150 V4.7	-			
			versions), SINAMICS				
			V4.7 SP1 (All versions				
			SINAMICS S150 V4.8	`			
			versions < V4.8 HF6),				
			SINAMICS S150 V5.1	`			
			versions), SINAMICS				
			V5.1 SP1 (All versions				
			SP1 HF4), SINAMICS	5210			
			V5.1 (All versions),				
			SINAMICS S210 V5.1	SP1			
			(All versions), SITOP				
			Manager (All versions	s),			
CV Scoring Sca	le 0.1	1.2	22 24 45		7.0	0.0	0.4
(CVSS)	0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-1

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SITOP PSU8600 (All versions), SITOP UPS1600 (All versions), TIM 1531 IRC (All versions). The webserver of the affected devices contains a vulnerability that may lead to a denial-of-service condition. An attacker may cause a denial-of-service situation which leads to a restart of the webserver of the affected device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.		
			CVE ID : CVE-2019-6568		
Improper Input Validation	17-04-2019	7.8	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP PC2 (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC NET PC Software (All versions), SIMATIC RF188C (All	N/A	A-SIE-SIMA- 010519/311

 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)	Publish Date	cvss	Description	& CVE ID	Pa	tch	NCIII	PC ID
			versions), SIMA	TIC RF600R				
			(All versions), S	SIMATIC S7-				
			1500 CPU famil	y (All				
			versions >= V2.	5), SIMATIC				
			S7-1500 Softwa	are Controller				
			(All versions >=	= V2.5),				
			SIMATIC WinCo	C OA (All				
			versions < V3.1	5-P018),				
			SIMATIC WinCo	C Runtime				
			Advanced (All v	versions),				
			SIMATIC WinCo	C Runtime				
			Comfort (All ve	rsions),				
			SIMATIC WinCo	C Runtime				
			HSP Comfort (A	all versions),				
			SIMATIC WinCo	C Runtime				
			Mobile (All vers	sions), SINEC-				
			NMS (All versio	ns), SINEMA				
			Server (All vers	sions),				
			SINUMERIK OP	C UA Server				
			(All versions <	V2.1),				
			TeleControl Ser	ver Basic (All				
			versions). Speci	ially crafted				
			network packet	-				
			affected devices					
			4840/tcp could	_				
			unauthenticate					
			attacker to caus	se a Denial-of-				
			Service condition	on of the OPC				
			communication					
			device. The seco					
			vulnerability co	-				
			exploited by an					
			network access					
			affected system					
			exploitation red					
			system privileg	•				
			user interaction					
			could use the vi					
			to compromise availability of					
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-1
(CVSS)	0.1	1 2	2 3 4	7 5 0	0-7	, 0	0-5	9-10

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			the ting public explosion vulnes	PC comme of ad cation no itation or rability of the comme	visory public f this se was kno	curity wn.				
simatic_s7-plo	csim_advance	d								
Improper Input Validation	17-04-2019	5	identi versio (All ve CP343 versio (All ve CP443 versio OPC U SIMA' Contr (All ve SIMA' Contr (All ve KTP7) und K SIMA' (All ve KTP7) und K SIMA' (All ve KTP1) und K SIMA' (All ve KTP1) und K SIMA' (All ve RF183 SIMA' versio (All ve	nerabilitified in Cons), CP1 ons), SIA ersions), 3-1 Adva ons), SIM ersions), 3-1 Adva ons), SIM IA (All vi FIC ET 2 oller CP ersions (ort Outd All versions), ort Outd All versions), ort Outd Comfort ersions), ort Outd Comfort ersions), ort Outd All versions), ort Outd All versions), ort Outd Ersions), ort Outd Ons), KTP2 Ons, KTP3 Ons), SIM ersions), ort Outd Ons), SIM ersions), ort Outd	P1604 (All ATIC RI ATIC CI ATIC RI ATI	(All ll ll F185C lC ll P443-1 lC ll P443-1 lC ll P6443-1 l, pen SP PC lC HMI lels 7" & MATIC lC HMI lC HMI lC HMI lC HMI lC HMI lC HMI lC lc hmi lC	N/A			SIMA- 9/312
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 Ty _l	pe(s): CSRF- Cross Denial of Service								nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			SIMA	ΓIC RF6	OOR (All					
				ns), SIM	•	7-1500				
				amily (A						
				лину (т. ГІС S7-1						
				oller (Al						
				гіс s7-3		-				
				ersions «						
			`	ΓΙC S7-4		-				
				d below	•	•				
				α <i>Β</i> C10W ΓΙC S7-4	•	-				
				F) (All v	•					
			`	ric S7-P	•	,				
				nced (Al		ie)				
				ΓIC Tele		13),				
				er IE Ad		(A11				
			^	ns), SIM		(All				
				ervice A		F Racic				
				ersions)	_					
			_	ervice A						
				ard (All	•					
				•						
				SIMATIC WinAC RTX 2010 (All versions), SIMATIC						
				C Runtin						
				ersions)						
			`	EIP (All						
			1	CODE pr		<i>,</i>				
				-		-				
				ns), SIN		3130				
			`	All vers	-	(A 11				
				MICS G1		•				
				ns), SIN						
				SP1 (All						
				MICS G1		(AII				
			versions < V4.8 HF6),							
			SINAMICS G130 V5.1 (All							
			versions), SINAMICS G130 V5.1 SP1 (All versions < V5.1							
				•						
				F4), SIN		1120				
			1	All vers	-	(
			SINAI	MICS G1	JU V4./	(AII				
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CV33)										

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Publish Date	cvss	De	scription & CVE	ID	Pat	tch	NCIII	PC ID
			versions	s), SINAMICS	G150				
			V4.7 SP:	1 (All version	s),				
			SINAMI	CS G150 V4.8	(All				
			versions	s < V4.8 HF6)					
			SINAMI	CS G150 V5.1	(All				
			versions	s), SINAMICS	G150				
			V5.1 SP	1 (All version	s < V5.1				
			SP1 HF4), SINAMICS	S120				
			V4.6 (Al	l versions),					
			SINAMI	CS S120 V4.7	(All				
			versions	s), SINAMICS	S120				
			V4.7 SP:	1 (All version	s),				
				CS S120 V4.8	-				
				s < V4.8 HF6)	-				
				CS S120 V5.1					
				s), SINAMICS	-				
				1 (All version					
), SINAMICS					
				l versions),					
			`	CS S150 V4.7	(All				
				s), SINAMICS	•				
				1 (All version					
				CS S150 V4.8	-				
				s < V4.8 HF6)	-				
				CS S150 V5.1					
				s), SINAMICS	-				
				1 (All version					
), SINAMICS					
				l versions),	3210				
			`	CS S210 V5.1	CD1				
					SF 1				
			-	sions), SITOP r (All version	a)				
					8),				
				SU8600 (All	1600				
				s), SITOP UPS					
			`	sions), TIM 15	31 IKC				
			`	sions). The					
				ver of the affe					
				contains a	1 1				
			vulnera	bility that ma	y lead				
CV Scoring Sca	le 0-1	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty									

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIII	PC ID
			to a denial-of-service condition. An attacker may cause a denial-of-service situation which leads to a restart of the webserver of the affected device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6568				
simatic_winco		anced					
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 Advanced (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2	N/A		A-SIE- 01051	SIMA- 9/313
CV Scoring Scal (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
Vulnerability Ty		_	uest Forgery; Dir. Trav Directory Tra oss Site Scripting; Sql- SQL Injection; I 203			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVI	E ID Pa	atch	NCIIF	PC ID
			(All versions), SIMAT	IC HMI			
			Comfort Outdoor Par	iels 7" &			
			15" (All versions), SI	MATIC			
			HMI Comfort Panels	4" - 22"			
			(All versions), SIMAT	'IC HMI			
			KTP Mobile Panels K	ГР400F,			
			KTP700, KTP700F, K	TP900			
			und KTP900F (All ve	rsions),			
			SIMATIC IPC DiagMo	nitor			
			(All versions), SIMAT	'IC			
			RF181-EIP (All version	ons),			
			SIMATIC RF182C (Al	l			
			versions), SIMATIC R	F186C			
			(All versions), SIMAT	'IC			
			RF188C (All versions),			
			SIMATIC RF600R (Al	ĺ			
			versions), SIMATIC S	7-1500			
			CPU family (All versi	ons),			
			SIMATIC S7-1500 So	ftware			
			Controller (All version	ns),			
			SIMATIC S7-300 CPU	-			
			(All versions < V3.X.1	.6),			
			SIMATIC S7-400 PN	incl. F)			
			V6 and below (All ve				
			SIMATIC S7-400 PN/				
			(incl. F) (All versions				
			SIMATIC S7-PLCSIM	,,			
			Advanced (All versio	ns).			
			SIMATIC Teleservice	-5,			
			Adapter IE Advanced	(All			
			versions), SIMATIC				
			Teleservice Adapter	E Basic			
			(All versions), SIMAT				
			Teleservice Adapter				
			Standard (All version				
			SIMATIC WinAC RTX	•			
			(All versions), SIMAT				
			WinCC Runtime Adva				
			(All versions), SIMO				
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-1
(CVSS) Vulnerability Ty					, ,		

Vulnerability Type(s)	Publish Date	cvss	De	scription & CVE	ID	Pa	tch	NCIII	PC ID
			pro V El	IP (All version	s),				
			SIMOCO	DE pro V PN	(All				
			version	s), SINAMICS	G130				
			V4.6 (A)	ll versions),					
			SINAMI	CS G130 V4.7	(All				
				s), SINAMICS	,				
				1 (All version:					
			SINAMI	CS G130 V4.8	(All				
			version	s < V4.8 HF6),	,				
				CS G130 V5.1					
				s), SINAMICS	•				
				1 (All version:					
				1), SINAMICS					
				ll versions),					
			_	CS G150 V4.7	(All				
				s), SINAMICS	•				
				1 (All version					
				CS G150 V4.8	-				
				s < V4.8 HF6),	,				
				CS G150 V5.1					
				s), SINAMICS	•				
				1 (All version					
				4), SINAMICS					
				ll versions),	3120				
			_	CS S120 V4.7	(All				
				s), SINAMICS	-				
				1 (All version					
				CS S120 V4.8					
				s < V4.8 HF6),	`				
				CS S120 V5.1					
				s), SINAMICS	`				
				1 (All version:					
				1 (All versions 4), SINAMICS					
				J.	3130				
			`	ll versions),	(A 11				
				CS S150 V4.7	`				
				s), SINAMICS :					
				1 (All versions					
				CS S150 V4.8 s < V4.8 HF6),	,				
CV Scoring Scal	le 0-1	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty		1-2	2-3	3-4 4-5	D-0	0-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	1	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			versice V5.1 SP1 H V5.1 (SINAN (All versice (All versice vulne to a device vulne vulne to a device vul	MICS S15 ons), SIN SP1 (All IF4), SIN (All vers MICS S2 ersions) ger (All P PSU86 ons), SIT ersions) erver of es conta rability enial-of- tion. An a denial ion which fected d ity vulne ploited b network ed syste itation r m privile nteracti use the mpromis evice. At ory public exploit ity vulne	AMICS Seversions (AMICS Security), 10 V5.1 (AMICS Security), SITOP (AMICS SECURITY), TIM 15 (AMI	S150 S < V5.1 S210 SP1 S), 1600 S1 IRC Cted y lead r may rice to a ver of he could acker to the cessful no no ttacker bility bility of e of no this				
			know CVE I	n. D : CVE -	2019-6	568				
Improper Input	17-04-2019	7.8	A vulnerability has been identified in SIMATIC				N/A			SIMA- 19/314
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descri	ption & CVE	ID	Pat	tch	NCIII	PC ID
Validation			CP443-1 0	PC UA (All					
			versions),	SIMATIC E	Γ 200				
			Open Cont	roller CPU	1515SP				
			PC2 (All ve	rsions), SII	MATIC				
			IPC DiagM	onitor (All					
			versions),	SIMATIC N	ET PC				
			Software (All versions	s),				
			SIMATIC R	F188C (All					
			versions),	SIMATIC RI	F600R				
			(All versio	ns), SIMAT	C S7-				
			1500 CPU	family (All					
			versions >	= V2.5), SIN	1ATIC				
			S7-1500 S						
				ns >= V2.5)					
			SIMATIC V	_					
			versions <	•					
			SIMATIC V						
			Advanced						
			SIMATIC V	-					
			Comfort (A						
			SIMATIC V						
			HSP Comfo						
			SIMATIC V	•	-				
			Mobile (Al						
			NMS (All v	-					
			`	,	INEMA				
			Server (All SINUMERI	-	ONLION				
					erver				
			(All versio	,	. (411				
			TeleContro		•				
			versions).						
			network p						
			affected de	•					
			4840/tcp						
			unauthent						
			attacker to						
			Service co						
			communic		ish the				
			device. The	_					
			vulnerabil	ty could be	!				
CV Scoring Scal	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross					_			

Type(s)	Publish Date	CVSS	l	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			netwo affect explo system user i could to cor the Ot the tin public explo vulne	PC comments of addition of the comments of the	eges and on. An avulnera e availa nunicati visory o public f this sewas kno	cessful no no ttacker bility bility of on. At curity wn.				
sitop_manage	3 7		CVE I	D : CVE-	2019-6	575				
Improper Input Validation	17-04-2019	5	identi versic (All versic (All versic (All versic (All versic OPC U SIMA' Contr (All versic (All versi	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2 (All versions), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions), SIMATIC HMI Comfort Panels 4" - 22" (All versions), SIMATIC HMI					A-SIE- 01051	SITO- 9/315
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)	Publish Date	cvss	Descriptio	n & CVE ID	Pa	tch	NCIII	PC ID
			und KTP900F	(All versions),				
			SIMATIC IPC D	DiagMonitor				
			(All versions),	SIMATIC				
			RF181-EIP (Al	l versions),				
			SIMATIC RF18	32C (All				
			versions), SIM	ATIC RF186C				
			(All versions),	SIMATIC				
			RF188C (All vo	ersions),				
			SIMATIC RF60	OR (All				
			versions), SIM	ATIC S7-1500				
			CPU family (Al	l versions),				
			SIMATIC S7-1	•				
			Controller (All	versions).				
			SIMATIC S7-3					
			(All versions <					
			SIMATIC S7-4	3 .				
			V6 and below	,				
			SIMATIC S7-4					
			(incl. F) (All ve	•				
			SIMATIC S7-P	•				
			Advanced (All					
			SIMATIC Teles	-				
			Adapter IE Ad					
			versions), SIM					
			-	lapter IE Basic				
			(All versions),					
			Teleservice Ad					
			Standard (All	•				
			SIMATIC Win	•				
			(All versions),					
			WinCC Runtim					
			(All versions),					
			pro V EIP (All	J .				
			SIMOCODE pr	•				
			versions), SIN					
			V4.6 (All versi	•				
			SINAMICS G13	•				
			versions), SIN. V4.7 SP1 (All v					
CV Scoring Scal	e e	1.3				7.0		
(CVSS)	0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pato	ch	NCIIF	PC ID
			SINAMICS G130 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS G130 V5.1 (All				
			versions), SINAMICS G130)			
			V5.1 SP1 (All versions < V	5.1			
			SP1 HF4), SINAMICS G150)			
			V4.6 (All versions),				
			SINAMICS G150 V4.7 (All				
			versions), SINAMICS G150)			
			V4.7 SP1 (All versions),				
			SINAMICS G150 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS G150 V5.1 (All				
			versions), SINAMICS G150)			
			V5.1 SP1 (All versions < V	5.1			
			SP1 HF4), SINAMICS S120				
			V4.6 (All versions),				
			SINAMICS S120 V4.7 (All				
			versions), SINAMICS \$120				
			V4.7 SP1 (All versions),				
			SINAMICS S120 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S120 V5.1 (All				
			versions), SINAMICS \$120				
			V5.1 SP1 (All versions < V				
			SP1 HF4), SINAMICS S150				
			V4.6 (All versions),				
			SINAMICS S150 V4.7 (All				
			versions), SINAMICS S150				
			V4.7 SP1 (All versions),				
			SINAMICS S150 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S150 V5.1 (All				
			versions), SINAMICS S150				
			V5.1 SP1 (All versions < V				
			SP1 HF4), SINAMICS S210				
			V5.1 (All versions),				
			SINAMICS S210 V5.1 SP1				
			(All versions), SITOP				
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-	6 6-7	7-8	8-9	9-1
(CVSS) Vulnerability Ty			5 ,		, ,	0 5	J 1

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
			situat restar the af securi be exp with r affect explorations system user i could to cont the de advise public securi know	evice. At ory puble exploit ity vulne	OO (All OP UPS: TIM 15 The the affectins a that may eservice attacker ch leads webserv evice. The erability oy an att access t ms. Succe equires eges and on. An a vulnera the time ication of erability	1600 31 IRC cted y lead r may rice to a ver of he could acker to the cessful no no ttacker bility bility of e of no this was				
simatic_winco	c_runtime_cor	nfort								
Improper Input Validation	17-04-2019	7.8	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP PC2 (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC NET PC				N/A			SIMA- 9/316
CV Scoring Scal (CVSS) Vulnerability Ty	e 0-1 pe(s): CSRF- Cross Denial of Service	_				-			8-9 nformatio	9-10 n; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			Softw	are (All	versions	s),				
			SIMA	TIC RF1	88C (All					
			versio	ons), SIM	IATIC RI	7600R				
			(All v	ersions)	, SIMATI	C S7-				
			1500	CPU fan	nily (All					
			versio	ons >= V	2.5), SIM	IATIC				
			S7-15	00 Softv	vare Cor	itroller				
			(All v	ersions	>= V2.5)	,				
			SIMA	TIC Win	CC OA (A	All				
			versio	ons < V3	.15-P01	3),				
			SIMA	TIC Win	CC Runt	me				
			Advai	nced (Al	l version	s),				
			SIMA	TIC Win	CC Runt	me				
			Comf	ort (All v	ersions),				
			SIMA	TIC Win	CC Runt	me				
			HSP (Comfort	(All vers	ions),				
			SIMA	TIC Win	CC Runt	me				
			Mobil	e (All ve	ersions),	SINEC-				
			NMS	(All vers	ions), SI	NEMA				
			Serve	r (All ve	rsions),					
			SINUI	MERIK C	PC UA S	erver				
			(All v	ersions ·	< V2.1),					
			TeleC	ontrol S	erver Ba	sic (All				
			versio	ons). Spe	cially cr	afted				
			netwo	ork pack	ets sent	to				
			affect	ed devic	es on po	rt				
			4840	tcp cou/	ld allow	an				
			unaut	henticat	ted remo	ote				
			attacl	er to ca	use a De	nial-of-				
			Servi	ce condi	tion of th	ne OPC				
			comn	nunicatio	on or cra	sh the				
			devic	e. The se	curity					
			vulne	rability	could be					
				•	ın attack					
			netwo	ork acce	ss to the					
			affect	ed syste	ms. Succ	essful				
				_	equires					
			syste	n privile	eges and	no				
				•	on. An at					
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty			2-5	5-4	4-3	3-0	0-7	7-0	0-3	5-10

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			to con the Ol the tin public explo- vulne CVE I	use the npromis PC comment of ad cation no itation or ability PC: CVE-	e availa nunicati visory o public f this se was kno	bility of on. At curity wn.				
simatic_winco	_runtime_hsp	o_comf	ort							
Improper Input Validation	17-04-2019	7.8	identi CP443 versice Open PC2 (A IPC Di versice Softw SIMA' versice S7-15 (All versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' versice SIMA' SIM	nerabilitication on San All versions), SIM are (All resions), SIM ersions), SIM ersions), SIM ersions >= V to 00 Software (All resions >= V to 10 C Windows (All resions), SIM ersions >= V to 10 C Windows (All resions), Ersions >= V to 10 C Windows (A	IMATIC UA (All IATIC ET er CPU ons), SIN tor (All IATIC NI Versions B8C (All IATIC RI ATIC RI ATIC RI ATIC RI ATIC RI CO (All	F 200 1515SP MATIC ET PC s), F600R IC S7- MATIC ntroller , All 8), ime is), ime sions), ime sions), ime SINEC- NEMA	N/A			-SIMA- 19/317
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	pe(s): CSRF- Cross Denial of Service	_				_				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patcl	h	NCIII	PC ID
			(All versions < V2.1), TeleControl Server Basic (All versions). Specially crafted network packets sent to affected devices on port 4840/tcp could allow an unauthenticated remote attacker to cause a Denial-of-Service condition of the OPC communication or crash the device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the OPC communication. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6575				
simatic_winco	runtime mo	hile	CVEID: CVE 2017 0070				
Improper Input Validation	17-04-2019	7.8	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP PC2 (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC NET PC Software (All versions), SIMATIC RF188C (All versions), SIMATIC RF600R	N/A		A-SIE- 01051	SIMA- 9/318
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Type		_	uest Forgery; Dir. Trav Directory Trav			formatio	n; DoS-
	Demai of Service	:, A33- Ur	oss Site Scripting; Sql- SQL Injection; N, 214	- мог Аррі	iicabie.		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	tch	NCIII	PC ID	
			(All versions), SIMATIC S7	-			
			1500 CPU family (All				
			versions >= V2.5), SIMATION	C			
			S7-1500 Software Controll	ler			
			(All versions >= V2.5),				
			SIMATIC WinCC OA (All				
			versions < V3.15-P018),				
			SIMATIC WinCC Runtime				
			Advanced (All versions),				
			SIMATIC WinCC Runtime				
			Comfort (All versions),				
			SIMATIC WinCC Runtime				
			HSP Comfort (All versions)),			
			SIMATIC WinCC Runtime				
			Mobile (All versions), SINE	EC-			
			NMS (All versions), SINEM	A			
			Server (All versions),				
			SINUMERIK OPC UA Serve	r			
			(All versions < V2.1),				
			TeleControl Server Basic (All			
			versions). Specially crafted				
			network packets sent to				
			affected devices on port				
			4840/tcp could allow an				
			unauthenticated remote				
			attacker to cause a Denial-	of-			
			Service condition of the OF				
			communication or crash th				
			device. The security				
			vulnerability could be				
			exploited by an attacker w	ith			
			network access to the	1011			
				.1			
			affected systems. Successfuexploitation requires no	uı			
			system privileges and no				
			user interaction. An attack	or			
			could use the vulnerability				
			to compromise availability the OPC communication. A				
CV Scoring Sca	e 0-1	1-2	2-3 3-4 4-5 5-6		7-8	8-9	9-10
(CVSS)	0-1	1-2	3-4 4-5 5-6	0-7	7-0	0-3	3-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID		Pa	itch	NCII	PC ID			
			the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6575								
sinec-nms											
Improper Input Validation	17-04-2019	7.8	SIMATIC WinCC OA (All versions < V3.15-P018), SIMATIC WinCC Runtime Advanced (All versions), SIMATIC WinCC Runtime Comfort (All versions), SIMATIC WinCC Runtime HSP Comfort (All versions), SIMATIC WinCC Runtime Mobile (All versions), SINEC- NMS (All versions), SINEC- NMS (All versions), SINEMA Server (All versions), SINUMERIK OPC UA Server (All versions < V2.1), TeleControl Server Basic (All versions). Specially crafted		N/A		A-SIE- 01051	SINE- 9/319			
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): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pate	ch	NCII	PC ID
			network packets sent to affected devices on port 4840/tcp could allow an unauthenticated remote attacker to cause a Denial-of- Service condition of the OPC communication or crash the device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the OPC communication. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6575				
sinema_serve	r		001101001111111111111111111111111111111				
Improper Input Validation	17-04-2019	7.8	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP PC2 (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC NET PC Software (All versions), SIMATIC RF188C (All versions), SIMATIC RF600R (All versions), SIMATIC S7-1500 CPU family (All versions >= V2.5), SIMATIC	N/A		A-SIE- 01051	SINE- 9/320
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
		_	uest Forgery; Dir. Trav Directory Trav oss Site Scripting; Sql- SQL Injection; N 217			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Desc	ription & CVE	ID	Pat	tch	NCIII	PCID			
			S7-1500	Software Cor	itroller							
			(All versi	ons >= V2.5)	,							
			SIMATIC	SIMATIC WinCC OA (All								
			versions	< V3.15-P018	3),							
			SIMATIC	WinCC Runti	me							
			Advanced	d (All version	s),							
			SIMATIC	WinCC Runti	me							
			Comfort	(All versions)),							
			SIMATIC	WinCC Runti	me							
			HSP Com	fort (All vers	ions),							
			SIMATIC	WinCC Runti	me							
			Mobile (A	all versions),	SINEC-							
			NMS (All	versions), SI	NEMA							
			Server (A	ll versions),								
			SINUMEF	RIK OPC UA S	erver							
			(All versi	ons < V2.1),								
			TeleCont	rol Server Ba	sic (All							
			versions)	. Specially cr	afted							
			network	packets sent	to							
			affected o	levices on po	rt							
			4840/tcp	could allow	an							
			unauther	iticated remo	ote							
			attacker t	to cause a De	nial-of-							
			Service co	ondition of th	ne OPC							
			communi	cation or cra	sh the							
			device. T	ne security								
			vulnerab	ility could be								
			exploited	by an attack	er with							
			network	access to the								
			affected s	ystems. Succ	essful							
			exploitati	on requires	no							
			system p	rivileges and	no							
				raction. An at								
			could use	the vulneral	oility							
			to compr	omise availal	oility of							
			the OPC o	ommunicati	on. At							
			the time	of advisory								
			publication	on no public								
			exploitati	ion of this se	curity							
CV Scoring Scal	e 0.1	1.2		4	ГС	6.7	7.0	0.0	0.40			
(CVSS)	pe(s): CSRF- Cross	1-2		-4 4-5	5-6	6-7	7-8	8-9	9-10			

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID	
			vulne	rability	was kno	wn.					
			CVE I	D : CVE-	2019-6	575					
telecontrol_se	erver_basic						•				
Improper Input Validation	17-04-2019	7.8	identi CP443 versic Open PC2 (A IPC Di versic Softw SIMA' versic ST-15 (All versic SIMA' Advar SIMA' Advar SIMA' Advar SIMA' Comfo SIMA' HSP C SIMA' Mobil NMS (Serve SINUM (All versic onetwo	nerability fied in S 3-1 OPC ons), SIM Control All versity iagMonity ons), SIM are (All FIC RF1: ons), SIM ersions) CPU fam ons >= V 00 Softw ersions : FIC Win ons < V3 FIC Win ons (All FIC Win ort (All w FIC W F	IMATIC UA (All IATIC E' ler CPU ons), SII tor (All IATIC NI IATIC NI IATIC NI IATIC NI IATIC NI IATIC RI IATIC	F 200 1515SP MATIC ET PC s), F600R IC S7- MATIC ntroller d, All 8), ime is), ime sions), ime SINEC- NEMA Gerver asic (All rafted to ort	N/A			-TELE- 19/321	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-											

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PC ID										
			attack Service commedevice vulne exploe network affect exploe system user if could to come the Off the time publice exploe vulne	ork accested syste itation reprivite methods in the privile use the	use a Decion of the curity could be an attack as to the ms. Succeedings and con. An acceeding a vulneration of this seconds as knowns as	enial-of- he OPC ash the exer with cessful no no ttacker bility bility of on. At curity wn.														
spectrum_pov	wer_4																			
N/A	17-04-2019	7.5	identi Powe Porta netwo serve 443/7 syster admir The so could unaut with r affect intera explo	nerabilithe in S r 4 (with al). An attempt access r on por access r acce	pectrum Web O cacker w ss to the t 80/TC d execut ands wi e privile rulnerab oited by ced attac access t ce. No us required curity	ffice ffice with web P or te th eges. oility an cker to the ser d to	N/A		A-SIE- 01051	SPEC- 9/322										
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10										
Vulnerability Ty	• • •	_				_			Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIIP	PC ID	
			vulne confic availa syster advise public secur know	itation of the control of the contro	comprongy, integrate the targetime of ication of artion of erability	mises rity or geted no this was					
siteserver			CVEI	D.CVE.	2019-0	3/9					
siteserver_cn	ns										
Unrestricted Upload of File with Dangerous Type	22-04-2019	6.5	SiteSe allow execu becau can ac exten conve	A issue was discovered in SiteServer CMS 6.9.0. It allows remote attackers to execute arbitrary code because an administrator can add the permitted file extension .aassp, which is converted to .asp because the "as" substring is deleted. CVE ID: CVE-2019-11401					A-SIT-9		
struktur											
libheif											
Use After Free	23-04-2019	6.8	free in heif::I heif::I heif_c heif_c refere alpha	libheif 1.4.0 has a use-after-free in heif::HeifContext::Image::set _alpha_channel in heif_context.h because heif_context.cc mishandles references to non-existing alpha images. CVE ID: CVE-2019-11471			N/A		A-STR- 01051		
supportcandy	y										
supportcandy											
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
· · · · · · · · · · · · · · · · · · ·	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
Unrestricted Upload of File with Dangerous Type	18-04-2019	7.5	Vulne Suppo throu allow execu uploa execu	restrict rability ortCandy gh 2.0.0 s remote te arbitr ding a fi table ex D: CVE-	in the plugin for Wor attacker ary cod le with a tension.	rdPress ers to e by an	N/A		A-SUP SUPP- 01051	
tabslab										
mailcarrier										
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2019	7.5	MailC remorarbitr string SMTP POP3 POP3	A buffer overflow in MailCarrier 2.51 allows remote attackers to execute arbitrary code via a long string, as demonstrated by SMTP RCPT TO, POP3 USER, POP3 LIST, POP3 TOP, or POP3 RETR. CVE ID: CVE-2019-11395					A-TAE MAIL- 01051	
urllib3_proje	ct									
urllib3										
Improper Certificate Validation	18-04-2019	5	1.24.2 misha where certification in situ verifications are corrected assl_co	The urllib3 library before 1.24.2 for Python mishandles certain cases where the desired set of CA certificates is different from the OS store of CA certificates, which results in SSL connections succeeding in situations where a verification failure is the correct outcome. This is related to use of the ssl_context, ca_certs, or ca_certs_dir argument.					A-URI URLL- 01051	
CV Scoring Scal	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(- ()))										

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID									
			CVE I	D : CVE-	2019-1	1324													
veronalabs																			
wp_statistics																			
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-04-2019	4.3	The WP Statistics plugin through 12.6.2 for WordPress has XSS, allowing a remote attacker to inject arbitrary web script or HTML via the Referer header of a GET request. CVE ID: CVE-2019-10864				ss has XSS, allowing attacker to inject web script or the Referer header request. statistics/wp statistics/co mmit/5aec0a 08680f0afea 387267a8d1			R- 19/328									
Verypdf																			
verypdf																			
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-04-2019	6.8	Overformann Execution pdfocution pdfed pdfcm	VeryPDF 4.1 has a Memory Overflow leading to Code Execution because pdfocx!CxImageTIF::operato r in pdfocx.ocx (used by pdfeditor.exe and pdfcmd.exe) is mishandled. CVE ID: CVE-2019-11493			N/A		A-VER VERY- 01051										
Vestacp																			
control_panel																			
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	19-04-2019	4.3	allow	Vesta Control Panel 0.9.8-23 allows XSS via a crafted URL. CVE ID: CVE-2019-9841		b.com, ey- rodin/ comm 5d29a 8110c	//githu /sergh /vesta/ it/c28c 3c61bc 11349 09cd53	A-VES CONT 01051											
W1.fi																			
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10									
vuillerability Ty		_				_			Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIII	PC ID	
hostapd											
Information Exposure	17-04-2019	4.3	in hose wpa_se vulne attack obserdiffer patter able trinformused for the control of the control	The implementations of SAE in hostapd and wpa_supplicant are vulnerable to side channel attacks as a result of observable timing differences and cache access patterns. An attacker may be able to gain leaked information from a side channel attack that can be used for full password recovery. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.7 are affected. CVE ID: CVE-2019-9494 The implementations of				//w1.fi rity/20	A-W1. HOST- 01051		
Use of a Broken or Risky Cryptographi c Algorithm	17-04-2019	4.3	EAP-I wpa_s vulne attack access of hos wpa_s PWD The a execu neces attack patter share passw Versio	PWD in he supplicates as a restand an supplicate support to te applicate applicate. Memore are well are words mare words are words mare words and words words are words and words are words are words and words are words are words and words are words are words and words are words	nt are side-cha esult of c as. All ve d are vulr install a cations i a succes ry access isible in Weak ay be cra	and annel ache ersions EAP- nerable. nd s ssful s a		//w1.fi ity/20	A-W1. HOST- 01051		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			and newer, are not vulnerable to the timing attack described in CVE-2019-9494. Both hostapd with EAP-pwd support and wpa_supplicant with EAP-pwd support prior to and including version 2.7 are affected. CVE ID: CVE-2019-9495		
Improper Authenticati on	17-04-2019	5	An invalid authentication sequence could result in the hostapd process terminating due to missing state validation steps when processing the SAE confirm message when in hostapd/AP mode. All version of hostapd with SAE support are vulnerable. An attacker may force the hostapd process to terminate, performing a denial of service attack. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.7 are affected. CVE ID: CVE-2019-9496	https://w1.fi /security/20 19-3/	A-W1 HOST- 010519/333
Improper Authenticati on	17-04-2019	6.8	The implementations of EAP-PWD in hostapd EAP Server and wpa_supplicant EAP Peer do not validate the scalar and element values in EAP-pwd-Commit. This vulnerability may allow an	https://w1.fi /security/20 19-4/	A-W1 HOST- 010519/334

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			attacker to complete EAP-PWD authentication without knowing the password. However, unless the crypto library does not implement additional checks for the EC point, the attacker will not be able to derive the session key or complete the key exchange. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.4 are affected. Both hostapd with EAP-pwd support and wpa_supplicant with EAP-pwd support of and including version 2.7 are affected. CVE ID: CVE-2019-9497		
N/A	17-04-2019	6.8	The implementations of EAP-PWD in hostapd EAP Server, when built against a crypto library missing explicit validation on imported elements, do not validate the scalar and element values in EAP-pwd-Commit. An attacker may be able to use invalid scalar/element values to complete authentication, gaining session key and network access without needing or learning the password. Both hostapd with SAE support and	https://w1.fi /security/20 19-4/	A-W1 HOST- 010519/335

Vulnerability Type(s)	Publish Da	ate CV	SS	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
				suppo include affecte EAP-p wpa_s pwd s include affecte		to and sion 2.4 hostape port and with prior to sion 2.7	are d with l EAP- and are				
N/A	17-04-20	19 6.8	}	The implementations of EAP-PWD in wpa_supplicant EAP Peer, when built against a crypto library missing explicit validation on imported elements, do not validate the scalar and element values in EAP-pwd-Commit. An attacker may complete authentication, session key and control of the data connection with a client. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.4 are affected. Both hostapd with EAP-pwd support and wpa_supplicant with EAP-pwd support to and including version 2.7 are affected.					//w1.fi rity/20	A-W1. HOST- 01051	
wpa_supplica	nt										
Information Exposure	17-04-20	19 4.3	3	The implementations of SAE https://in hostapd and /securi						A-W1. WPA_	
CV Scoring Scal (CVSS)	0-1	1-2		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- (Denial of Se						_			ntormatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			wpa_supplicant are vulnerable to side channel attacks as a result of observable timing differences and cache access patterns. An attacker may be able to gain leaked information from a side channel attack that can be used for full password recovery. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.7 are affected. CVE ID: CVE-2019-9494	19-1/	010519/337
Use of a Broken or Risky Cryptographi c Algorithm	17-04-2019	4.3	The implementations of EAP-PWD in hostapd and wpa_supplicant are vulnerable to side-channel attacks as a result of cache access patterns. All versions of hostapd and wpa_supplicant with EAP-PWD support are vulnerable. The ability to install and execute applications is necessary for a successful attack. Memory access patterns are visible in a shared cache. Weak passwords may be cracked. Versions of hostapd/wpa_supplicant 2.7 and newer, are not vulnerable to the timing attack described in CVE-	https://w1.fi /security/20 19-2/	A-W1 WPA 010519/338

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			2019-9494. Both hostapd with EAP-pwd support and wpa_supplicant with EAP-pwd support prior to and including version 2.7 are affected. CVE ID: CVE-2019-9495		
Improper Authenticati on	17-04-2019	5	An invalid authentication sequence could result in the hostapd process terminating due to missing state validation steps when processing the SAE confirm message when in hostapd/AP mode. All version of hostapd with SAE support are vulnerable. An attacker may force the hostapd process to terminate, performing a denial of service attack. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.7 are affected. CVE ID: CVE-2019-9496	https://w1.fi /security/20 19-3/	A-W1 WPA 010519/339
Improper Authenticati on	17-04-2019	6.8	The implementations of EAP-PWD in hostapd EAP Server and wpa_supplicant EAP Peer do not validate the scalar and element values in EAP-pwd-Commit. This vulnerability may allow an attacker to complete EAP-PWD authentication without knowing the password.	https://w1.fi /security/20 19-4/	A-W1 WPA 010519/340

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			However, unless the crypto library does not implement additional checks for the EC point, the attacker will not be able to derive the session key or complete the key exchange. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.4 are affected. Both hostapd with EAP-pwd support and wpa_supplicant with EAP-pwd support and including version 2.7 are affected. CVE ID: CVE-2019-9497		
N/A	17-04-2019	6.8	The implementations of EAP-PWD in hostapd EAP Server, when built against a crypto library missing explicit validation on imported elements, do not validate the scalar and element values in EAP-pwd-Commit. An attacker may be able to use invalid scalar/element values to complete authentication, gaining session key and network access without needing or learning the password. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.4 are	https://w1.fi /security/20 19-4/	A-W1 WPA 010519/341

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			EAP-p wpa_s pwd s includ	ed. Both owd sup supplica support ling vers ed. D: CVE-	port and nt with I prior to sion 2.7	l EAP- and are				
N/A	17-04-2019	6.8	EAP-F EAP P a cryp explication validateleme Comp session the da client SAE si wpa_s support include affects EAP-p wpa_s pwd s include affects	mplement of the property of the set of the s	vpa_supen built ry missintion on nents, decalar and es in EAR etacker in nentication destaped version with to and sion 2.4 hostape port and prior to sion 2.7	plicant against against against onot d P-pwd- may ion, ol of with a with SAE are d with EAP- and are		//w1.fi rity/20	A-W1. WPA_ 01051	
Wavpack										
Wavpack										
Access of Uninitialized Pointer	24-04-2019	4.3	WavpackSetConfiguration64 in pack_utils.c in libwavpack.a in WavPack through 5.1.0 has a				N/A		A-WAY WAVP 01051	
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 Typ	pe(s): CSRF- Cross Denial of Service	_							nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	IPC ID
			deper value might cause (appli file th	ditional jads on ual condition allow a denial ication contact lacks lata. D: CVE-	ninitialis on, which ttackers of servin rash) vis valid san	sed ch to ice a a DFF mple-				
wcms										
wcms										
Unrestricted Upload of File with Dangerous Type	20-04-2019	6.5	p in W Arbita Vulne devel .php i accor fm_ge	s/wex/fi VCMS v0 rary File rability oper/fin s a valid ding to t et_text_e D: CVE-	.3.2 has Upload via der beca extension he xts funct	ause on tion.	N/A		A-WC WCMS 01051	
whatsns										
whatsns										
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	22-04-2019	7.5	index html	sns 4.0 a .php?qu title SQL D : CVE -	estion/a injectio	n.	N/A		A-WH WHAT 01051	
Improper Neutralizatio n of Special Elements used in an	22-04-2019	6.5	index qid S(whatsns 4.0 allows index.php?inform/add.html qid SQL injection. CVE ID: CVE-2019-11451			N/A		A-WH WHA7 01051	
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cro Denial of Servi	_				_				on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descr	iption & CVE	ID	Pa	tch	NCII	PC ID
SQL Command ('SQL Injection')									
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	22-04-2019	6.5	emove.htn injection.	.0 allows Padmin_cate nl cid[] SQL VE-2019-1		N/A		A-WH WHAT 01051	
wifi_ftp_serve	er_project								
wifi_ftp_serve	er								
N/A	22-04-2019	5	An issue was discovered in the Medha WiFi FTP Server application 1.8.3 for Android. An attacker can read the username/password of a valid user via /data/data/com.medhaapps. wififtpserver/shared_prefs/com.medhaapps.wififtpserve r_preferences.xml CVE ID: CVE-2019-11383		N/A			F-WIFI- 19/348	
wordfence									
wordfence									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	25-04-2019	4.3	The Wordfence plugin 7.2.3 for WordPress allows XSS via a unique attack vector. CVE ID: CVE-2019-9669			N/A		A-WO WORI 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4		5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE II) Patch	NCIIPC ID
Scripting')					
zalora				,	
zalora					
N/A	22-04-2019	5	The Zalora application for Android stores confidential information insecurely on the system plain text), which allow non-root user to find on username/password or valid user via /data/data/com.zalora oid/shared_prefs/login xml.	n m (i.e. rs a ut the f a N/A	A-ZAL- ZALO- 010519/350
			CVE ID : CVE-2019-11	384	
Zohocorp					
servicedesk_p	olus				
Session Fixation	24-04-2019	6.5	Zoho ManageEngine ServiceDesk 9.3 allows session hijacking and privilege escalation bed an established guest se is automatically conver into an established administrator session with guest user enters the administrator username with an arbitrary incompassword, in an mc/lo attempt within a different browser tab. CVE ID: CVE-2019-10	https://www .manageengi ne.com/prod ucts/service- desk/readme .html	A-ZOH- SERV- 010519/351
manageengin	e application	s mana			
Improper Neutralizatio	22-04-2019	10	An issue was discovere Zoho ManageEngine	d in https://www .manageengi	A-ZOH- MANA-
CV Scoring Scal (CVSS)	0-1	1-2	2-3 3-4 4-5 uest Forgery; Dir. Trav Direct	5-6 6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			Applications Manager 11.0 through 14.0. An unauthenticated user can gain the authority of SYSTEM on the server due to a Popup_SLA.jsp sid SQL injection vulnerability. For example, the attacker can subsequently write arbitrary text to a .vbs file. CVE ID: CVE-2019-11448	ne.com/prod ucts/applicat ions_manage r/security- updates/secu rity-updates- cve-2019- 11448.html	010519/352
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	23-04-2019	10	Zoho ManageEngine Applications Manager 12 through 14 allows FaultTemplateOptions.jsp resourceid SQL injection. Subsequently, an unauthenticated user can gain the authority of SYSTEM on the server by uploading a malicious file via the "Execute Program Action(s)" feature.	https://www .manageengi ne.com/prod ucts/applicat ions_manage r/security- updates/secu rity-updates- cve-2019- 11469.html	A-ZOH- MANA- 010519/353
			CVE ID : CVE-2019-11469		
			Operating System		
ABB					
pm554-tp-eth	1_firmware				
Uncontrolled Resource Consumption	17-04-2019	5	ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO - Programmable Logic Controllers, multiple versions. Researchers have found some controllers are susceptible to a denial-of- service attack due to a flood of network packets.	N/A	O-ABB- PM55- 010519/354
	lo la				
CV Scoring Scal (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			CVE I	D : CVE-	2019-1	0953				
Canonical									_	
ubuntu_linux										
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-04-2019	6.4	files, I versic 7.2.x I below read I exif_p functi inforr crash.	PHP EXITORS 7.1.x pelow 7. y 7.3.4 cast allo rocess_I on. This mation d	F extens below 7 2.17 and an be cau cated bu FD_TAG may lea isclosur	sion in 7.1.28, d 7.3.x used to affer in ad to re or	N/A		N- - 19/355	
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-04-2019	6.4	When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in exif_iif_add_value function. This may lead to information disclosure or crash.				N/A		0-CAN UBUN 01051	
			CVE I	D : CVE-	2019-1	1035				
Use After Free	18-04-2019	5	found and ir which sensit leaked	-after-from the control of the could record of	maker u version esult in rmation system	2.0.1 certain to be logs.	N/A		0-CAN UBUN 01051	
centos-webpa	nel		CVLI	DI OVE	_01/ 0	300				
centos_web_p	<u> </u>		ContC	C-Mohn	and cor	n (alza			O-CEN	J_
Improper Neutralizatio	18-04-2019	3.5		S-WebP CentOS		•	N/A		CENT-	
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_				-				on; DoS-

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	itch	NCI	IPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Version is vulta Stored Admir "CWP Setting Change XSS Passe Capage Capag	0.9.8.793 (Free/Open Source Version) and 0.9.8.753 (Pro) is vulnerable to Stored/Persistent XSS for Admin Email fields on the "CWP Settings > "Edit Settings" screen. By changing the email ID to any XSS Payload and clicking on Save Changes, the XSS Payload will execute. CVE ID: CVE-2019-10893				0105	19/358	
Ciago			CVEI	D : CVE-	2019-1	0893				
Cisco aironet_acces	es point firm	wana								
				nerabilit						
Improper Input Validation	17-04-2019	5.5	of service (QoS) feature of Cisco Aironet Series Access Points (APs) could allow an authenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation on QoS fields within Wi-Fi frames by the affected device. An attacker could exploit this vulnerability by sending malformed Wi-Fi frames to an affected device. A successful exploit could allow the attacker to cause the affected device to crash, resulting in a DoS condition. CVE ID: CVE-2019-1826				N/A			-AIRO- 19/359
Improper Authenticati	17-04-2019	7.2		nerabilit Aironet			N/A		O-CIS	-AIRO-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6				6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cros Denial of Servic	_	_			_			nformatio	on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
on			Points (APs) could allow an authenticated, local attacker to gain access to the underlying Linux operating system (OS) without the proper authentication. The attacker would need valid administrator device credentials. The vulnerability is due to improper validation of usersupplied input for certain CLI commands. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input for a CLI command. A successful exploit could allow the attacker to obtain access to the underlying Linux OS without proper authentication. CVE ID: CVE-2019-1829		010519/360
Improper Input Validation	17-04-2019	3.3	A vulnerability in the internal packet processing of Cisco Aironet Series Access Points (APs) could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected AP if the switch interface where the AP is connected has port security configured. The vulnerability exists because the AP forwards some malformed	N/A	O-CIS-AIRO- 010519/361

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			wireless client packets outside of the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel. An attacker could exploit this vulnerability by sending crafted wireless packets to an affected AP. A successful exploit could allow the attacker to trigger a security violation on the adjacent switch port, which could result in a DoS condition. Note: Though the Common Vulnerability Scoring System (CVSS) score corresponds to a High Security Impact Rating (SIR), this vulnerability is considered Medium because a workaround is available and exploitation requires a specific switch configuration. There are workarounds that address this vulnerability. CVE ID: CVE-2019-1834		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-04-2019	2.1	A vulnerability in the CLI of Cisco Aironet Access Points (APs) could allow an authenticated, local attacker to access sensitive information stored in an AP. The vulnerability is due to improper sanitization of user-supplied input in specific CLI commands. An attacker could exploit this vulnerability by accessing	N/A	O-CIS-AIRO- 010519/362

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CVE	ID	Pat	tch	NCIIP	CID
			the CLI of an affected AP with administrator privileges and issuing crafted commands that result in directory traversal. A successful exploit could allow the attacker to view system files on the affected device, which could contain sensitive information. Software versions 8.8 and 8.9 are affected. CVE ID: CVE-2019-1835						
			CVE ID : CV	E-2019-1	835				
ios_xr			A 1 1.		TCD				
Improper Access Control	17-04-2019	5	A vulnerability flags inspectaccess controlled access controlled access controlled access controlled access controlled agregation. Routers could unauthentic attacker to be protection of configured affected devial affected devial access and affected for an affected of an affected cisco Expressional balance tuple hash a enabled. An exploit this sending traffected devial affected devial affected devial access acces	cion feature of lists (A 2000 Series of Services of allow a steed, removed attention of the control of the cont	re for CLs) on some of the of the rface when ding he 3-sould ity by he an analytical to the ould by the	N/A		O-CIS-1 01051	_
CV Scoring Scal	_								

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to bypass protection offered by a configured ACL on the affected device. There are workarounds that address this vulnerability. Affected Cisco IOS XR versions are: Cisco IOS XR Software Release 5.1.1 and later till first fixed. First Fixed Releases: 6.5.2 and later, 6.6.1 and later. CVE ID: CVE-2019-1686		
Improper Input Validation	17-04-2019	5	A vulnerability in the Event Management Service daemon (emsd) of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper handling of gRPC requests. An attacker could exploit this vulnerability by repeatedly sending unauthenticated gRPC requests to the affected device. A successful exploit could cause the emsd process to crash, resulting in a DoS condition. Resolved in Cisco IOS XR 6.5.1 and later.	N/A	O-CIS-IOS 010519/364
Improper Input Validation	17-04-2019	5	A vulnerability in the Protocol Independent Multicast (PIM) feature of	N/A	O-CIS-IOS 010519/365

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause the PIM process to restart, resulting in a denial of service condition on an affected device. The vulnerability is due to the incorrect processing of crafted AutoRP packets. An attacker could exploit this vulnerability by sending crafted packets to port UDP 496 on a reachable IP address on the device. A successful exploit could allow the attacker to cause the PIM process to restart. Software versions prior to 6.2.3, 6.3.2, 6.4.0, and 6.5.1 are affected. CVE ID: CVE-2019-1712		
Debian					
debian_linux					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	19-04-2019	4.3	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {},) because of Object.prototype pollution. If an unsanitized source object contained an enumerableproto property, it could extend the native Object.prototype. CVE ID: CVE-2019-11358	N/A	O-DEB- DEBI- 010519/366

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)	Publish Date	cvss	I	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
Dlink							l.			
di-524_firmw	are									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-04-2019	3.5	On D-Link DI-524 V2.06RU devices, multiple Stored and Reflected XSS vulnerabilities were found in the Web Configuration: /spap.htm, /smap.htm, and /cgi-bin/smap, as demonstrated by the cgi-bin/smap RC parameter. CVE ID: CVE-2019-11017			N/A		0-DLI- 01051	_	
Fedoraprojec	·+		CVEI	D: CVE	-2019-1	1017				
	.t									
fedora	T			1 5 7776 1	2 2	0.10				
Improper Authenticati on	22-04-2019	7.5	does in reflect spoof "Drag similate 9497.	not previous for ing, aka onblood	l" issue, to CVE-2	of ication a 2019-	N/A		0-FED FEDO- 01051	
Insufficient Verification of Data Authenticity	22-04-2019	7.5	FreeRADIUS before 3.0.19 mishandles the "each participant verifies that the received scalar is within a range, and that the received group element is a valid point on the curve being used" protection mechanism, aka a "Dragonblood" issue, a similar issue to CVE-2019-9498 and CVE-2019-9499. CVE ID: CVE-2019-11235			N/A		0-FED FEDO- 01051		
Use After	18-04-2019	5	A use-after-free flaw was				N/A		O-FED	-
CV Scoring Scal										
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Free			found in pacemaker up to and including version 2.0.1 which could result in certain sensitive information to be leaked via the system logs. CVE ID: CVE-2019-3885		FEDO- 010519/370
N/A	17-04-2019	6.8	The implementations of EAP-PWD in hostapd EAP Server, when built against a crypto library missing explicit validation on imported elements, do not validate the scalar and element values in EAP-pwd-Commit. An attacker may be able to use invalid scalar/element values to complete authentication, gaining session key and network access without needing or learning the password. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.4 are affected. Both hostapd with EAP-pwd support and wpa_supplicant with EAP-pwd support of and including version 2.7 are affected.	https://w1.fi /security/20 19-4/	O-FED- FEDO- 010519/371
N/A	17-04-2019	6.8	The implementations of EAP-PWD in wpa_supplicant EAP Peer, when built against a crypto library missing	https://w1.fi /security/20 19-4/	O-FED- FEDO- 010519/372

Vulnerability Type(s)	Publish Date	cvss	Description	on & CVE I	D	Pa	tch	NCIIF	PCID
			explicit validatimported element value commit. An a complete authorized session key at the data connclient. Both he SAE support awpa_supplication support priorincluding versaffected. Both EAP-pwd support including versaffected. CVE ID: CVE	ments, do calar and es in EAP ttacker mentication de contro ection with S to and sion 2.4 a hostapd port and nt with E prior to a sion 2.7 a sion 2.7 a	-pwd- nay on, ol of ith a ith AE with AP- and				
Google android									
N/A	19-04-2019	4.6	In updateAssi of Editor.java possible escape Setup Wizard missing perm This could lead escalation of FRP bypass wadditional exceptivileges need interaction is exploitation. AndroidVersi 8.0Android II 120866126	there is pe from to due to a ission change or ivilege with no ecution eded. Use not need froduct: ons: And	a he eck. l and r ed for	e.andr m/sec	//sourc oid.co urity/b /2019-	0-G00 ANDR- 01051	
CV Scoring Scal	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

(CVSS) Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			CVE I	D : CVE-	2019-2	026				
Out-of- bounds Write	19-04-2019	9.3	out of an inc This c code of additi privile intera explose Andro 7.0 Ar 7.1.2 A 8.1 Ar A-119	floor 0.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-119120561. CVE ID: CVE-2019-2027 In numerous hand-crafted				//sourc oid.co urity/b /2019-	O-GOC ANDR- 01051	
Improper Input Validation	19-04-2019	9.3	functi regist This c code e additi privile intera exploi Andro 7.0 Ar 7.1.2 A 8.1 Ar				e.andr m/sec	//sourc oid.co urity/b /2019-	0-G00 ANDR- 01051	
Use After Free	19-04-2019	6.8	In btm_proc_smp_cback of tm_ble.cc, there is a possible memory corruption due to a use after free. This could lead to remote code			tm_ble.cc, there is a possible memory corruption due to a use after free. This could		//sourc oid.co urity/b /2019-	0-G0C ANDR- 01051	
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_	_			_			itormatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-120612744. CVE ID: CVE-2019-2029		
Use After Free	19-04-2019	7.5	In removeInterfaceAddress of NetworkController.cpp, there is a possible use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-119496789.	https://sourc e.android.co m/security/b ulletin/2019- 04-01	O-GOO- ANDR- 010519/377
Out-of- bounds Write	19-04-2019	4.6	In rw_t3t_act_handle_check_nd ef_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android- 7.0 Android-7.1.1 Android- 7.1.2 Android-8.0 Android- 8.1 Android-9. Android ID:	https://sourc e.android.co m/security/b ulletin/2019- 04-01	O-GOO- ANDR- 010519/378

Vulnerability Type(s)	Publish Date	cvss	Description &	CVE ID	Patch	NCIIP	C ID
			A-120502559.				
			CVE ID : CVE-201	9-2031			
Out-of- bounds Write	19-04-2019	4.6	In SetScanRespond ble_advertiser_hcit cc, there is a possi bound write due to bounds check. This lead to local escalar privilege with no a execution privilege. User interaction is needed for exploit Product: Android-8.0 Android-8.0 Android-9. Android-9. Android-121145627.	_interface. ble out-of- o a missing s could ation of http additional es needed. anot ulle ration. Versions: oid-8.1	os://sourc droid.co security/b tin/2019- 01	O-GOO ANDR- 010519	
			CVE ID : CVE-201	9-2032			
Use After Free	19-04-2019	4.6	additional execution privileges needed. User interaction is not needed for		os://sourc droid.co security/b tin/2019- 01	0-G00 ANDR- 010519	
Out-of- bounds Write	19-04-2019	6.8	In rw_i93_sm_read rw_i93.cc, there is out-of-bounds wri an integer overflow could lead to local of privilege in the process with no ad execution privilege	a possible te due to e.an m/s escalation NFC 04-0	os://sourc droid.co security/b tin/2019- 01	O-GOO ANDR- 010519	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-	5 5-6 6-7	7-8	8-9	9-10

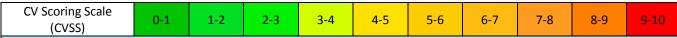
Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-122035770. CVE ID: CVE-2019-2034		
Out-of- bounds Write	19-04-2019	6.8	In rw_i93_sm_update_ndef of rw_i93.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-122320256 CVE ID: CVE-2019-2035	https://sourc e.android.co m/security/b ulletin/2019- 04-01	O-GOO- ANDR- 010519/382
Out-of- bounds Read	19-04-2019	5	In l2cu_send_peer_config_rej of l2c_utils.cc, there is a possible out-of-bound read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0	https://sourc e.android.co m/security/b ulletin/2019- 04-01	O-GOO- ANDR- 010519/383

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Android-8.1 Android-9. Android ID: A-119870451.		
			CVE ID : CVE-2019-2037		
Out-of- bounds Read	19-04-2019	4.3	In rw_i93_process_sys_info of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-121259048.	https://sourc e.android.co m/security/b ulletin/2019- 04-01	0-G00- ANDR- 010519/384
			CVE ID : CVE-2019-2038		
Out-of- bounds Read	19-04-2019	4.7	In rw_i93_sm_detect_ndef of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-121260197. CVE ID: CVE-2019-2039	https://sourc e.android.co m/security/b ulletin/2019- 04-01	O-GOO- ANDR- 010519/385
Out-of-	19-04-2019	4.7	In	https://sourc	O-GOO- ANDR-
CV Scoring Scal	e o	1.3	rw_i93_process_ext_sys_info		
	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
bounds Read			of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-122316913. CVE ID: CVE-2019-2040	m/security/b ulletin/2019- 04-01	010519/386
N/A	19-04-2019	6.9	In the configuration of NFC modules on certain devices, there is a possible failure to distinguish individual devices due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-8.1 Android-9. Android ID: A-122034690. CVE ID: CVE-2019-2041	https://sourc e.android.co m/security/b ulletin/2019- 04-01	O-GOO- ANDR- 010519/387
IBM					
bladecenter_l	ns23_firmwar	e			
Improper Input Validation	22-04-2019	7.8	A potential vulnerability was found in an SMI handler in various BIOS versions of certain legacy IBM System x and IBM BladeCenter systems that could lead to denial of service.	N/A	O-IBM- BLAD- 010519/388

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID			Patch		NCIIPC ID		
			CVE ID : CVE-2019-6155							
system_x3530_m4_firmware										
Improper Input Validation	22-04-2019	7.8	A potential vulnerability was found in an SMI handler in various BIOS versions of certain legacy IBM System x and IBM BladeCenter systems that could lead to denial of service. CVE ID: CVE-2019-6155			N/A		O-IBM-SYST- 010519/389		
system_x3630_m4_firmware										
Improper Input Validation	22-04-2019	7.8	A potential vulnerability was found in an SMI handler in various BIOS versions of certain legacy IBM System x and IBM BladeCenter systems that could lead to denial of service. CVE ID: CVE-2019-6155		N/A		O-IBM-SYST- 010519/390			
system_x3650	D_m4_hd_firm	ware								
Improper Input Validation	22-04-2019	7.8	A potential vulnerability was found in an SMI handler in various BIOS versions of certain legacy IBM System x and IBM BladeCenter systems that could lead to denial of service. CVE ID: CVE-2019-6155		N/A		O-IBM-SYST- 010519/391			
intelbras										
iwr_3000n_fii	rmware									
Weak Password Recovery Mechanism for Forgotten	ssword covery echanism 22-04-2019 4.		An issue was discovered on Intelbras IWR 3000N 1.5.0 devices. When the administrator password is changed from a certain client				N/A		O-INT-IWR 010519/392	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; SqI- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Password			IP address, administrative authorization remains available to any client at that IP address, leading to complete control of the router.		
Improper Input Validation	22-04-2019	7.8	An issue was discovered on Intelbras IWR 3000N 1.5.0 devices. A malformed login request allows remote attackers to cause a denial of service (reboot), as demonstrated by JSON misparsing of the \""} string to v1/system/login. CVE ID: CVE-2019-11415	N/A	O-INT-IWR 010519/393
Cross-Site Request Forgery (CSRF)	22-04-2019	9.3	A CSRF issue was discovered on Intelbras IWR 3000N 1.5.0 devices, leading to complete control of the router, as demonstrated by v1/system/user. CVE ID: CVE-2019-11416	N/A	O-INT-IWR 010519/394
Linux					
linux_kernel					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	23-04-2019	6.9	The Siemens R3964 line discipline driver in drivers/tty/n_r3964.c in the Linux kernel before 5.0.8 has multiple race conditions. CVE ID: CVE-2019-11486	N/A	O-LIN-LINU- 010519/395



Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; Dos-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
miui					
miui					
N/A	18-04-2019	2.1	A vulnerability was found in the MIUI OS version 10.1.3.0 that allows a physically proximate attacker to bypass Lockscreen based authentication via the Wallpaper Carousel application to obtain sensitive Clipboard data and the user's stored credentials (partially). This occurs because of paste access to a social media login page. CVE ID: CVE-2019-11015	N/A	O-MIU-MIUI- 010519/396
Motorola			CVE ID : CVE-2019-11015		
m2_firmware			1. 1.		
Improper Neutralizatio n of Special Elements used in a Command ('Command Injection')	18-04-2019	7.5	An issue was discovered in Motorola CX2 1.01 and M2 1.01. There is a command injection in the function downloadFirmware in hnap, which leads to remote code execution via shell metacharacters in a JSON value.	N/A	O-MOT- M2_F- 010519/397
			CVE ID : CVE-2019-11319		
N/A	18-04-2019	7.5	In Motorola CX2 1.01 and M2 1.01, users can access the router's /priv_mgt.html web page to launch telnetd, as demonstrated by the 192.168.51.1 address. CVE ID: CVE-2019-11320	N/A	O-MOT- M2_F- 010519/398

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1			J .	. 5	3 0	Ŭ,	, 0	U J	J 10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	18-04-2019 5 without authentication to obtain information such as the MAC addresses of connected client devices. CVE ID: CVE-2019-11321		N/A	O-MOT- M2_F- 010519/399	
Improper Neutralizatio n of Special Elements used in a Command ('Command Injection')	18-04-2019	7.5	An issue was discovered in Motorola CX2 1.01 and M2 1.01. There is a command injection in the function startRmtAssist in hnap, which leads to remote code execution via shell metacharacters in a JSON value. CVE ID: CVE-2019-11322	N/A	O-MOT- M2_F- 010519/400
cx2_firmware	<u> </u>				
Improper Neutralizatio n of Special Elements used in a Command ('Command Injection')	18-04-2019	7.5	An issue was discovered in Motorola CX2 1.01 and M2 1.01. There is a command injection in the function downloadFirmware in hnap, which leads to remote code execution via shell metacharacters in a JSON value. CVE ID: CVE-2019-11319	N/A	O-MOT- CX2 010519/401
N/A	18-04-2019	7.5	In Motorola CX2 1.01 and M2 1.01, users can access the router's /priv_mgt.html web page to launch telnetd, as demonstrated by the	N/A	O-MOT- CX2 010519/402

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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; Dos-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			192.1	68.51.1	address.					
			CVE I	D : CVE-	2019-1	1320				
Information Exposure	18-04-2019	5	Motor 1.01. port 8 hnap withou obtain the M conne	rola CX2 The rout 8010. Us requests out authe a inform AC addr ected clie	1.01 and the open ers can see to this entication ation suresses of ent device.	d M2 s TCP send port n to ch as	N/A	N/A		Γ- 9/403
			An iss	sue was	discover	ed in				
Improper Neutralizatio n of Special Elements used in a Command ('Command Injection')	18-04-2019	7.5	Motor 1.01. inject startF which execu metac value	An issue was discovered in Motorola CX2 1.01 and M2 1.01. There is a command injection in the function startRmtAssist in hnap, which leads to remote code execution via shell metacharacters in a JSON value. CVE ID: CVE-2019-11322			N/A		O-MO7 CX2 01051	Γ- 9/404
Oracle										
solaris										
Improper Access Control	23-04-2019	2.1	Solari Sun S (subc Servio versio Easily vulne privil logon where	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: File Locking Services). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise		N/A		0-0RA SOLA- 01051	4- 9/405	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).		
			CVE ID: CVE-2019-2577 Vulnerability in the Oracle Solaris component of Oracle		
Information Exposure	23-04-2019	5	Sun Systems Products Suite (subcomponent: IPS Package Manager). The supported version that is affected is 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	N/A	O-ORA- SOLA- 010519/406
Phoenixconta	ct		CVE ID : CVE-2019-2704		
ilc_151_eth_fir					

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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	Description &	Pat	tch	NCII	PC ID	
Uncontrolled Resource Consumption	17-04-2019	5	ABB, Phoenix Con Schneider Electric WAGO - Program Logic Controllers, versions. Research found some control susceptible to a deservice attack due of network packet CVE ID: CVE-201	N/A)-ILC 9/407	
Redhat								
virtualization	l							
N/A	22-04-2019	4.3	A memory leak in archive_read_form anup in archive_read_suppt_zip.c in libarchive allows remote attacause a denial of some a crafted ZIP file be HAVE_LZMA_H typthis only affects us downloaded the development code GitHub. Users of the product?s official are unaffected. CVE ID: CVE-201	port_forma e 3.3.4-dev ackers to ervice via ecause of a po. NOTE: sers who e from ne releases	N/A		O-RED VIRT- 01051)- 9/408
enterprise_lin	ıux							
Improper Authenticati on	22-04-2019	7.5	FreeRADIUS before does not prevent to reflection for authorizing, aka a "Dragonblood" issuinilar issue to CV 9497.	N/A		O-RED ENTE- 01051		
CV Scoring Scal (CVSS)	0-1	1-2 Site Reg	2-3 3-4 4-		6-7	7-8	8-9	9-10 n: DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11234		
Insufficient Verification of Data Authenticity	22-04-2019	7.5	FreeRADIUS before 3.0.19 mishandles the "each participant verifies that the received scalar is within a range, and that the received group element is a valid point on the curve being used" protection mechanism, aka a "Dragonblood" issue, a similar issue to CVE-2019-9498 and CVE-2019-9499. CVE ID: CVE-2019-11235	N/A	O-RED- ENTE- 010519/410
Schneider-ele	ectric				
modicon_m22	21_firmware				
Uncontrolled Resource Consumption	17-04-2019	5	ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO - Programmable Logic Controllers, multiple versions. Researchers have found some controllers are susceptible to a denial-of- service attack due to a flood of network packets. CVE ID: CVE-2019-10953	N/A	O-SCH- MODI- 010519/411
Siemens					·
simatic_rf600	r_firmware				
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 Advanced (All	N/A	O-SIE-SIMA- 010519/412
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
(CVSS) Vulnerability Ty	• • • •	_	uest Forgery; Dir. Trav Directory Trav.oss Site Scripting; Sql- SQL Injection; N,		

Vulnerability Type(s)	Publish Date	cvss	Descri	tion & CVE	ID	Pat	tch	NCIII	PC ID
			versions), S	IMATIC CI	P443-1				
			OPC UA (Al	versions)	,				
			SIMATIC E	200 SP O	pen				
			Controller	CPU 1515S	SP PC				
			(All version	s < V2.1.6),				
			SIMATIC E						
			Controller CPU 1515SP PC2						
			(All version	s), SIMAT	IC HMI				
			Comfort Outdoor Panels 7" &						
			15" (All versions), SIMATIC						
			HMI Comfo	rt Panels 4	-" - 22"				
			(All version	s), SIMAT	IC HMI				
			KTP Mobile	Panels K7	P400F,				
			KTP700, K	'P700F, K	ГР900				
			und KTP90	0F (All ver	sions),				
			SIMATIC IP	C DiagMor	nitor				
			(All version	s), SIMAT	IC				
			RF181-EIP	(All versio	ns),				
			SIMATIC R	182C (All	-				
			versions), S	IMATIC R	F186C				
			(All version	s), SIMAT	IC				
			RF188C (A	l versions),				
			SIMATIC R						
			versions), S	IMATIC S7	7-1500				
			CPU family	(All versio	ns),				
			SIMATIC S7						
			Controller	All version	ns),				
			SIMATIC S7	•					
			(All version		-				
			SIMATIC ST		J .				
			V6 and belo	•	,				
			SIMATIC ST	•	-				
			(incl. F) (Al	•					
			SIMATIC S7						
			Advanced (All versions), SIMATIC Teleservice						
			Adapter IE Advanced (All versions), SIMATIC						
			Teleservice		E Basic				
CV Scoring Scale	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross								

Vulnerability Type(s)	Publish Date	cvss	Descri	ption & CVE	ID	Pat	tch	NCIII	PCID
			(All version	ns), SIMAT	IC				
			Teleservic	Adapter I	E				
			Standard (All version	s),				
			SIMATIC W	inAC RTX	2010				
			(All version	ns), SIMAT	IC				
			WinCC Rur						
			(All version	rs), SIMOC	ODE				
			pro V EIP (All version	s),				
			SIMOCODE	pro V PN	(All				
			versions),	SINAMICS (G130				
			V4.6 (All v	ersions),					
			SINAMICS	G130 V4.7	(All				
			versions),	SINAMICS (G130				
			V4.7 SP1 (A	All versions	s),				
			SINAMICS	G130 V4.8	(All				
			versions <	V4.8 HF6),					
			SINAMICS	G130 V5.1	(All				
			versions),	SINAMICS (G130				
			V5.1 SP1 (A	All versions	s < V5.1				
			SP1 HF4),	SINAMICS (G150				
			V4.6 (All v	ersions),					
			SINAMICS	G150 V4.7	(All				
			versions),	SINAMICS (G150				
			V4.7 SP1 (A	All versions	s),				
			SINAMICS	G150 V4.8	(All				
			versions <	V4.8 HF6),					
			SINAMICS	G150 V5.1	(All				
			versions),	SINAMICS (G150				
			V5.1 SP1 (A	All versions	s < V5.1				
			SP1 HF4),	SINAMICS S	S120				
			V4.6 (All v	ersions),					
			SINAMICS	S120 V4.7	(All				
			versions),		•				
			V4.7 SP1 (A						
			SINAMICS						
			versions < V4.8 HF6),						
			SINAMICS						
			versions), SINAMICS S120						
			V5.1 SP1 (All versions < V5.1						
CV Scoring Scale	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross					_			

Vulnerability Type(s)	Publish Date	cvss	Description	n & CVE ID	Pa	tch	NCIII	PC ID
			SP1 HF4), SINA	AMICS S150				
			V4.6 (All version	ons),				
			SINAMICS S15	0 V4.7 (All				
			versions), SINA	AMICS S150				
			V4.7 SP1 (All v	ersions),				
			SINAMICS S15	0 V4.8 (All				
			versions < V4.8	3 HF6),				
			SINAMICS S15	0 V5.1 (All				
			versions), SINA	AMICS S150				
			V5.1 SP1 (All v	ersions < V5.1				
			SP1 HF4), SINA	AMICS S210				
			V5.1 (All version	ons),				
			SINAMICS S21	0 V5.1 SP1				
			(All versions),	SITOP				
			Manager (All v	ersions),				
			SITOP PSU860	0 (All				
			versions), SITC	OP UPS1600				
			(All versions),	TIM 1531 IRC				
			(All versions).	The				
			webserver of t	he affected				
			devices contain	ns a				
			vulnerability tl	hat may lead				
			to a denial-of-s					
			condition. An a	ittacker may				
			cause a denial-	of-service				
			situation whicl	h leads to a				
			restart of the w	vebserver of				
			the affected de	vice. The				
			security vulner	rability could				
			be exploited by	•				
			with network a					
			affected systen					
			exploitation re					
			system privileg	-				
			user interactio					
			could use the v					
			to compromise	-				
			the device. At t	-				
			advisory publi					
CV Scoring Sca	e 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-1
(CVSS)	0-1	1-2	2-3 3-4	4-5	0-7	7-0	0-3	3-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6568		
Improper Input Validation	17-04-2019	7.8	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP PC2 (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC NET PC Software (All versions), SIMATIC RF600R (All versions), SIMATIC RF600R (All versions), SIMATIC S7-1500 CPU family (All versions >= V2.5), SIMATIC S7-1500 Software Controller (All versions >= V2.5), SIMATIC WinCC OA (All versions < V3.15-P018), SIMATIC WinCC Runtime Advanced (All versions), SIMATIC WinCC Runtime Comfort (All versions), SIMATIC WinCC Runtime Comfort (All versions), SIMATIC WinCC Runtime HSP Comfort (All versions), SIMATIC WinCC Runtime HSP Comfort (All versions), SIMATIC WinCC Runtime Mobile (All versions), SINECNMS (All versions), SINEMA Server (All versions), SINEMA Server (All versions), SINEMA Server (All versions), SINUMERIK OPC UA Server (All versions). Specially crafted network packets sent to affected devices on port	N/A	O-SIE-SIMA- 010519/413

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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; Dos-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIII	PC ID
			4840/tcp could allow an unauthenticated remote attacker to cause a Denial-of-Service condition of the OPC communication or crash the device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the OPC communication. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6575				
simatic_s7-15	600_firmware		CVE ID . CVE Z017 0373				
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 Advanced (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2			O-SIE- 01051	_
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	• • • •	_	uest Forgery; Dir. Trav Directory Travoss Site Scripting; Sql- SQL Injection; N 264			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CV	E ID Pa	atch	NCIII	PC ID		
			(All versions), SIMA	ГІС НМІ					
			Comfort Outdoor Pa	nels 7" &					
			15" (All versions), Sl	MATIC					
			HMI Comfort Panels						
			(All versions), SIMA'	ГІС НМІ					
			KTP Mobile Panels k	TP400F,					
			KTP700, KTP700F, F	TP900					
			und KTP900F (All ve	ersions),					
			SIMATIC IPC DiagMo						
			(All versions), SIMA						
			RF181-EIP (All versi						
			SIMATIC RF182C (A	•					
			versions), SIMATIC I						
			(All versions), SIMA						
			RF188C (All version						
			SIMATIC RF600R (A	-					
			versions), SIMATIC S						
			CPU family (All vers						
			SIMATIC S7-1500 Sc	-					
			Controller (All versions),						
			SIMATIC S7-300 CPU family (All versions < V3.X.16),						
			SIMATIC S7-400 PN	-					
			V6 and below (All ve	`					
			SIMATIC S7-400 PN	-					
			·						
			(incl. F) (All versions SIMATIC S7-PLCSIM	5),					
			Advanced (All version	-					
			SIMATIC Teleservice						
			Adapter IE Advance	i (All					
			versions), SIMATIC						
			Teleservice Adapter						
			(All versions), SIMA						
			Teleservice Adapter						
			Standard (All versio						
			SIMATIC WinAC RTX						
			(All versions), SIMA						
			WinCC Runtime Adv						
			(All versions), SIMO	CODE					
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-1		
(CVSS)	0.1	1 2	2 3 4 4-3	3 0 0-7	, 0	3 3)-1		

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE	ID	Pa	tch	NCIII	PC ID
			pro V EIP (Al	l version:	s),				
			SIMOCODE p	ro V PN (All				
			versions), SII	NAMICS (130				
			V4.6 (All vers	sions),					
			SINAMICS G1	30 V4.7 (All				
			versions), SII	NAMICS (130				
			V4.7 SP1 (All	versions),				
			SINAMICS G1	30 V4.8 (All				
			versions < V	l.8 HF6),					
			SINAMICS G1	30 V5.1 (All				
			versions), SII	NAMICS (130				
			V5.1 SP1 (All	versions	< V5.1				
			SP1 HF4), SII	NAMICS C	150				
			V4.6 (All vers	sions),					
			SINAMICS G1	50 V4.7 (All				
			versions), SII	NAMICS C	150				
			V4.7 SP1 (All	versions),				
			SINAMICS G1	50 V4.8 (All				
			versions < V	l.8 HF6),					
			SINAMICS G1	50 V5.1 (
			versions), SII	NAMICS (
			V5.1 SP1 (All	versions					
			SP1 HF4), SII						
			V4.6 (All vers						
			SINAMICS S1		All				
			versions), SII	`					
			V4.7 SP1 (All						
			SINAMICS S1		,				
			versions < V	`					
			SINAMICS S1		All				
			versions), SII	`					
			V5.1 SP1 (All						
			SP1 HF4), SII						
			V4.6 (All vers						
			SINAMICS S1		All				
			versions), SII	`	'				
			V4.7 SP1 (All						
			SINAMICS S1						
		versions < V							
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-1
(CVSS)	V 1		5 4		5 5	0,	, 0		

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			SINAN	AICS S1	50 V5.1	(All				
			versio	ns), SIN	AMICS S	S150				
			V5.1 S	SP1 (All	versions	s < V5.1				
			SP1 H	F4), SIN	AMICS S	5210				
			`	All vers						
			_		10 V5.1	SP1				
			-	ersions)						
			•	•	versions	s),				
				PSU86	•					
				-	OP UPS:					
			`	,	, TIM 15	31 IRC				
			`	ersions)						
					the affeo	cted				
				es conta						
					that may	lead				
				enial-of-						
					attackei	•				
					l-of-serv					
			situation which leads to a restart of the webserver of the affected device. The							
					evice. Ti erability					
				-	y an att					
			_		access t					
					ms. Suc					
				-	equires					
			•		eges and					
			_	•	on. An a					
					vulnera					
						bility of				
				•	the time	•				
			adviso	ory publ	ication i	10				
					ation of					
			_	-	erability					
			know	•	J					
			CVE ID : CVE-2019-6568							
Improper	17.04.2010	7.0	A vulr	nerabilit	y has be	en	NI / A		O-SIE-	SIMA-
Input	17-04-2019	7.8			IMATIC		N/A		01051	9/415
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross	Site Req	uest Forg	gery; Dir. 1	rav Dire	ctory Trav	ersal; +In	fo- Gain II	nformatio	n: DoS-

Vulnerability Type(s)	Publish Date	cvss	Descri	ption & CVE	ID	Pat	tch	NCIII	PC ID	
Validation			CP443-1 0	PC UA (All						
			versions),	SIMATIC E	Γ 200					
			Open Cont	roller CPU	1515SP					
			PC2 (All ve	rsions), SII	MATIC					
			IPC DiagM	onitor (All						
			versions),	SIMATIC N	ET PC					
			Software (All versions	s),					
			SIMATIC R	F188C (All						
			versions),	SIMATIC RI	F600R					
			(All versio	ns), SIMAT	C S7-					
			1500 CPU	family (All						
			versions >	= V2.5), SIN	IATIC					
			S7-1500 S							
				ns >= V2.5)						
			SIMATIC V	_						
			versions <	•						
			SIMATIC V							
			Advanced							
			SIMATIC V	-						
			Comfort (A							
			`							
			SIMATIC WinCC Runtime HSP Comfort (All versions),							
				•	CC Runtime					
			`	Mobile (All versions), SINEC- NMS (All versions), SINEMA						
			`	,	INEMA					
			Server (All SINUMERI	-	ONLION					
					erver					
			(All versio	,	. (411					
			TeleContro		•					
			versions).							
			network p							
			affected de	•						
			4840/tcp							
			unauthent							
			attacker to							
			Service co							
			communic		ish the					
			device. The	_						
			vulnerabil	ty could be	!					
CV Scoring Scal	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10	
(CVSS)	pe(s): CSRF- Cross									

Improper Input Validation 17-04-			netwo affector explored system user in could to cont the Ol the time public explored vulner	ork accessed systemitation reprivite use the empromise PC comments of additation or ability of the emproments of the empronents of the emproments of the emproments of the emp	ms. Succeequires needed and responsible and responsible available or public of this security was knowns	essful o no cacker ility ility of n. At				
Improper Input 17-04-				D : CVE-		v 11.				
Improper Input 17-04					2019-65	75				
Input 17-04-			identi	fied in C	y has bee					
	-2019	5	version (All versi	ons), SIA ersions), 3-1 Adva ons), SIM ersions), 3-1 Adva ons), SIM JA (All versions < Comparison of Comparisons), ort Outd All versions), Mobile Pa	MTIC RF: , SIMATIC anced (Alimatic CPa , SIMATIC anced (Alimatic CPa ersions), 00 SP Op U 1515SF V2.1.6), 00 SP Op U 1515SF , SIMATIC oor Panel ons), SIMATIC anels 4" , SIMATIC anels KTF	E 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	N/A		O-SIE- 01051	
CV Scoring Scale (CVSS)			2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	D	escriptio	n & CVE	ID	Pa	tch	NCII	PC ID
			und K	ΓP900F	(All ver	sions),				
			SIMAT	IC IPC D	iagMon	itor				
			(All ve	rsions),	SIMATI	C				
			RF181	-EIP (Al	versio	ns),				
			SIMAT	IC RF18	2C (All					
			versio	ns), SIM.	ATIC RE	F186C				
			(All ve	rsions),	SIMATI	C				
			RF188	C (All ve	rsions)	,				
			SIMAT	IC RF60	OR (All					
			versio	ns), SIM	ATIC S7	-1500				
			CPU fa	mily (Al	l versio	ns),				
			SIMAT	IC S7-15	00 Soft	ware				
			Contro	ller (All	versior	ıs),				
			SIMAT	IC S7-30	00 CPU	family				
			(All ve	rsions <	V3.X.16	ó),				
			SIMAT	IC S7-40	00 PN (i	ncl. F)				
			V6 and	l below	All ver	sions),				
			SIMAT	IC S7-40	00 PN/I	OP V7				
			(incl. F) (All ve	rsions)	,				
			SIMAT	IC S7-PI	LCSIM					
			Advan	ced (All	version	s),				
			SIMATIC Teleservice							
			Adapter IE Advanced (All							
			Adapter IE Advanced (All versions), SIMATIC							
			Telese	rvice Ad	apter II	E Basic				
				rsions),						
			Telese	rvice Ad	apter II	Ξ				
			Standa	rd (All v	ersions	s),				
			SIMAT	IC WinA	C RTX 2	2010				
			(All ve	rsions),	SIMATI	C				
			WinCC	Runtim	e Advai	nced				
			(All ve	rsions),	SIMOCO	ODE				
			-	EIP (All						
			_	ODE pro		-				
				ns), SINA	•	•				
				All versi						
			SINAMICS G130 V4.7 (All							
				ns), SIN		•				
				P1 (All v						
CV Scoring Scale	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Tyr	pe(s): CSRF- Cross		uest Forge	erv: Dir. Tı	av Dire	ctory Tray	ersal: +Int	o- Gain In	formatio	n: DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pato	ch	NCIIF	PC ID	
			SINAMICS G130 V4.8 (All					
			versions < V4.8 HF6),					
			SINAMICS G130 V5.1 (All					
			versions), SINAMICS G130)				
			V5.1 SP1 (All versions < V	5.1				
			SP1 HF4), SINAMICS G150)				
			V4.6 (All versions),					
			SINAMICS G150 V4.7 (All					
			versions), SINAMICS G150)				
			V4.7 SP1 (All versions),					
			SINAMICS G150 V4.8 (All					
			versions < V4.8 HF6),					
			SINAMICS G150 V5.1 (All					
			versions), SINAMICS G150)				
			V5.1 SP1 (All versions < V	5.1				
			SP1 HF4), SINAMICS S120					
			V4.6 (All versions),					
			SINAMICS S120 V4.7 (All					
			versions), SINAMICS \$120					
			V4.7 SP1 (All versions),					
			SINAMICS S120 V4.8 (All					
			Versions < V4.8 HF6),					
			SINAMICS S120 V5.1 (All					
			versions), SINAMICS \$120					
			V5.1 SP1 (All versions < V					
			SP1 HF4), SINAMICS S150					
			V4.6 (All versions),					
			SINAMICS S150 V4.7 (All					
			versions), SINAMICS S150					
			V4.7 SP1 (All versions),					
			SINAMICS S150 V4.8 (All					
			versions < V4.8 HF6),					
			SINAMICS S150 V5.1 (All					
			versions), SINAMICS S150					
			V5.1 SP1 (All versions < V					
			SP1 HF4), SINAMICS S210					
			V5.1 (All versions),					
			SINAMICS S210 V5.1 SP1					
			(All versions), SITOP					
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-	6 6-7	7-8	8-9	9-1	
(CVSS) Vulnerability Ty			5 ,		, ,	0 5	J 1	

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			situate to a device vulne to a device vulne to a de condi cause situate restare the affecte exploresystem user in could to continue de advise public securities.	evice. At ory publ c exploit ity vulne	OO (All OP UPS: TIM 15 The the affectins a chat may service attacker -of-serv ch leads webserv evice. The crability y an att access t ms. Succe equires eges and on. An access t the time ication of crability	1600 31 IRC cted r lead r may rice to a rer of ne could acker to the cessful no no ttacker bility bility of e of no this was				
cp1616_firmv	vare								•	
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC				N/A			-CP16- -9/417
CV Scoring Scal (CVSS) Vulnerability Ty	e 0-1 pe(s): CSRF- Cross Denial of Service	_	_			_			8-9 nformatio	9-10 n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
			CP443-1 Advanced (All				
			versions), SIMATIC CP443-	1			
			OPC UA (All versions),				
			SIMATIC ET 200 SP Open				
			Controller CPU 1515SP PC				
			(All versions < V2.1.6),				
			SIMATIC ET 200 SP Open				
			Controller CPU 1515SP PC2				
			(All versions), SIMATIC HM	I			
			Comfort Outdoor Panels 7"	&			
			15" (All versions), SIMATIC				
			HMI Comfort Panels 4" - 22				
			(All versions), SIMATIC HM	I			
			KTP Mobile Panels KTP400				
			KTP700, KTP700F, KTP900	•			
			und KTP900F (All versions)				
			SIMATIC IPC DiagMonitor	"			
			(All versions), SIMATIC				
			RF181-EIP (All versions),				
			SIMATIC RF182C (All				
			versions), SIMATIC RF1860				
			(All versions), SIMATIC	'			
			RF188C (All versions),				
			SIMATIC RF600R (All				
			•				
			versions), SIMATIC S7-1500				
			CPU family (All versions), SIMATIC S7-1500 Software				
			Controller (All versions),				
			SIMATIC S7-300 CPU family	7			
			(All versions < V3.X.16),	.			
			SIMATIC S7-400 PN (incl. F				
			V6 and below (All versions)	,			
			SIMATIC S7-400 PN/DP V7				
			(incl. F) (All versions),				
			SIMATIC S7-PLCSIM				
			Advanced (All versions),				
			SIMATIC Teleservice				
		Adapter IE Advanced (All					
			versions), SIMATIC				
CV Scoring Sca	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		
(CVSS)	0-1	1-2	2-3 3-4 4-3 3-6	7-8	0-9 9-10		

Vulnerability Type(s)	Publish Date	cvss	Desc	ription & CVE	ID	Par	tch	NCIII	PC ID
			Teleservi	ce Adapter II	E Basic				
				ons), SIMATI					
			Teleservi	ce Adapter II	Ξ				
				(All versions					
			SIMATIC	WinAC RTX	2010				
			(All version	ons), SIMATI	С				
			`	ıntime Adva					
			(All version	ons), SIMOCO	ODE				
			-	(All version					
			-	E pro V PN (-				
				, SINAMICS (
			V4.6 (All						
			=	G130 V4.7	(All				
				, SINAMICS (-				
				(All versions					
				G130 V4.8					
				< V4.8 HF6),	(AII				
				5 G130 V5.1	(
					-				
			-	, SINAMICS (
				(All versions					
			-	, SINAMICS (
			V4.6 (All	_					
				G150 V4.7	-				
			-	, SINAMICS (
				(All versions					
				G150 V4.8	(All				
				< V4.8 HF6),					
				G150 V5.1	`				
			versions)	, SINAMICS (G150				
			V5.1 SP1	(All versions	< V5.1				
			SP1 HF4)	, SINAMICS S	120				
			V4.6 (All	versions),					
			SINAMICS	S S120 V4.7 (All				
			versions)	, SINAMICS S	120				
			V4.7 SP1	(All versions),				
			SINAMICS	S S120 V4.8 (All				
			versions <	< V4.8 HF6),					
			SINAMICS	S S120 V5.1 (All				
				, SINAMICS S	-				
CV Scoring Sca	le								
(CVSS)	0-1	1-2	2-3 3	-4 4-5	5-6	6-7	7-8	8-9	9-1

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			V5.1 S	P1 (All	versions	s < V5.1				
				•	AMICS S					
			V4.6 (All vers	ions),					
			SINAN	IICS S1	50 V4.7	(All				
			versio	ns), SIN	AMICS S	S150				
			V4.7 S	P1 (All	versions	s),				
				•	50 V4.8					
					.8 HF6),	-				
					50 V5.1					
					AMICS S	•				
				-	versions					
				•	AMICS S					
				All vers						
			`		10 V5.1	SP1				
				ersions)		31 1				
			`		versions	:)				
			1	PSU86		,,,				
					OP UPS:	1600				
				-						
			(All versions), TIM 1531 IRC (All versions). The webserver of the affected devices contains a							
						, load				
				_	that may ·service	/ Ieau				
					attackei	,				
					l-of-serv					
					ch leads					
					webserv	-				
					evice. Tl					
				-	erability					
			_		y an att					
			-		access t					
				-	ms. Suc					
			exploi	tation r	equires	no				
			_	•	eges and					
			user ii	nteracti	on. An a	ttacker				
			could use the vulnerability							
			to con	npromis	se availa	bility of				
			the de	vice. At	the time	e of				
CV Scoring Sca	le	1.2	2.2	2.4	4.5	Г.С	6.7	7.0	0.0	0.10
(CVSS) Vulnerability Ty	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss		Descriptio	on & CVE	ID	Pa	tch	NCI	IPC ID
			public securi know	ory puble exploit ty vulne n. D : CVE-	ation of erability	this was				
simatic_cp343	3-1_advanced	_firmw	are							
Improper Input Validation	17-04-2019	5	identi versic versic (All ve CP343 versic (All ve CP443 versic OPC U SIMA' Contr (All ve SIMA' Contr (All ve KTP N KTP7 und K SIMA' (All ve RF183 SIMA' versic (All ve	nerability fied in Cons), CP1 ons), SIA ersions), B-1 Adva ons), SIM ersions), B-1 Adva ons), SIM IA (All versions), ort Outd All versions), ort Outd All versions), ort Outd Comfort ersions), ort Outd TIC ET 2 oller CP ersions, ort Outd All versions), ort Outd Comfort ersions), ort Outd	P1604 (All MTIC RIANCED (ALL MTIC RIANCED (ALL MTIC CITES) (ALL MTIC RIANCED (ALL MT	(All I I F185C IC IC II F185C IC II F186C IC	N/A			-SIMA- 19/418
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 Typ	pe(s): CSRF- Cross Denial of Service	_	_	-		_			nformatio	on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	ID	Pa	tch	NCIII	PC ID	
			versions), S	IMATIC S7	'-1500					
			CPU family	(All versio	ns),					
			SIMATIC S7	-1500 Sof	tware					
			Controller (All version	ıs),					
			SIMATIC S7	-300 CPU	family					
			(All version	s < V3.X.1	6),					
			SIMATIC S7	-400 PN (1	ncl. F)					
			V6 and belo	w (All ver	sions),					
			SIMATIC S7	-400 PN/I	OP V7					
			(incl. F) (Al	l versions)	,					
			SIMATIC S7	-PLCSIM						
			Advanced (All version	ıs),					
			SIMATIC Te	eleservice						
			Adapter IE	Advanced	(All					
			versions), S	IMATIC						
			Teleservice	Adapter I	E Basic					
			(All version	s), SIMAT	C					
			Teleservice	-						
			Standard (A	All version:	s),					
		SIMATIC WinAC RTX 2010								
			(All version	s), SIMAT	C					
			WinCC Run							
			(All version	s), SIMOC	ODE					
			_	(All versions),						
			SIMOCODE	pro V PN (All					
			versions), S	_						
			V4.6 (All ve							
			SINAMICS ((All					
			versions), S		`					
			V4.7 SP1 (A							
			SINAMICS (
			versions < \		(
			SINAMICS (-	(All					
			versions), S							
			V5.1 SP1 (A							
			SP1 HF4), S							
			V4.6 (All ve		1100					
			SINAMICS G150 V4.7 (All							
			versions), S		`					
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	0.1	
(CVSS)	0-1	1-2	2-3 3-4	4-5	3-0	0-7	7-0	0-9	9-1	

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
			V4.7 SP1 (All versions),					
			SINAMICS G150 V4.8 (All					
			versions < V4.8 HF6),					
			SINAMICS G150 V5.1 (All					
			versions), SINAMICS G150					
			V5.1 SP1 (All versions < V5.1	1				
			SP1 HF4), SINAMICS S120					
			V4.6 (All versions),					
			SINAMICS S120 V4.7 (All					
			versions), SINAMICS S120					
			V4.7 SP1 (All versions),					
			SINAMICS S120 V4.8 (All					
			versions < V4.8 HF6),					
			SINAMICS S120 V5.1 (All					
			versions), SINAMICS S120					
			V5.1 SP1 (All versions < V5.1	1				
			SP1 HF4), SINAMICS S150					
			V4.6 (All versions),					
			SINAMICS S150 V4.7 (All					
			versions), SINAMICS S150					
			V4.7 SP1 (All versions),					
			SINAMICS S150 V4.8 (All					
			versions < V4.8 HF6),					
			SINAMICS S150 V5.1 (All					
			versions), SINAMICS S150					
			V5.1 SP1 (All versions < V5.1	1				
			SP1 HF4), SINAMICS S210					
			V5.1 (All versions),					
			SINAMICS S210 V5.1 SP1					
			(All versions), SITOP					
			•					
			Manager (All versions),					
			SITOP PSU8600 (All					
			versions), SITOP UPS1600	,				
			(All versions), TIM 1531 IR(•				
			(All versions). The					
			webserver of the affected					
			devices contains a					
			vulnerability that may lead					
	<u> </u>		to a denial-of-service					
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-1			
(CVSS) Vulnerability Ty								

			cause situati restar the aff	tion. An a denial ion which tof the	l-of-serv	•				
			be exp with r affector explois system user in could to con the de- advisor public	ity vulned be bloited be bloited be bloited be bloited by steed system of the bloited by	webserverice. The rability by an attaccess to ms. Succession. An avulnerace availathe time ication of	rer of ne could acker o the cessful no no ttacker bility bility of e of no this				
simptic and 12.1	1 advanced	firm		D : CVE-	2019-6	568				
Validation	7-04-2019	_firmw	A vulridenti versio (All versio (All versio OPC USIMATICALL CONTROLL CONTRO	nerability fied in Cons), CP1 ons), SIA ersions), 3-1 Adva ons), SIM JA (All vo TIC ET 2 oller CP1 ersions < color cp1 ersions,	CP1604 (Ale (Ale (Ale (Ale (Ale (Ale (Ale (Ale	All I F185C IC Ill P443-1 IC Ill P443-1 pen P PC I),	N/A		0-SIE- 01051	SIMA- 9/419
CV Scoring Scale (CVSS) Vulnerability Type(1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descripti	on & CVE ID	Pa	tch	NCIII	PC ID
			Comfort Outo	loor Panels 7"	&			
			15" (All versi	ons), SIMATIC				
			=	Panels 4" - 22				
			(All versions)	, SIMATIC HM	I			
			`	anels KTP400				
			KTP700, KTP	700F, KTP900				
			·	F (All versions)				
			SIMATIC IPC	DiagMonitor				
			(All versions)	· ·				
			RF181-EIP (<i>A</i>					
			SIMATIC RF1	J .				
				AATIC RF186C				
			(All versions)					
			RF188C (All v					
			SIMATIC RF6	-				
				ИАТІС S7-150()			
			CPU family (A					
			• •	1500 Software				
			Controller (A					
			-	300 CPU family	,			
			(All versions	•				
			`	< v 5.x.10), 100 PN (incl. F)	,			
				(All versions)	,			
				100 PN/DP V7				
			(incl. F) (All v					
			SIMATIC S7-I					
			Advanced (Al	,				
			SIMATIC Tele					
			Adapter IE A					
			versions), SIN					
				dapter IE Basi	С			
			(All versions)					
			Teleservice A	•				
			Standard (All	versions),				
			SIMATIC Win	AC RTX 2010				
			(All versions)					
			WinCC Runti	me Advanced				
			(All versions)	, SIMOCODE				
			pro V EIP (Al	l versions),				
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	D	escriptio	n & CVE	ID	Pa	tch	NCIII	PC ID
			SIMOC	ODE pr	o V PN (All				
			versio	ns), SIN	AMICS (G130				
			V4.6 (A	All versi	ons),					
			SINAM	IICS G13	30 V4.7	(All				
			versio	ns), SIN	AMICS (G130				
			V4.7 S	P1 (All v	ersions	s),				
			SINAM	IICS G13	30 V4.8	(All				
			versio	ns < V4.	8 HF6),					
			SINAM	IICS G13	30 V5.1	(All				
			versio	ns), SIN	AMICS (G130				
			V5.1 S	P1 (All v	ersions	s < V5.1				
			SP1 HI	F4), SIN	AMICS (G150				
			V4.6 (A	All versi	ons),					
			SINAM	IICS G15	50 V4.7	(All				
			versio	ns), SIN	AMICS (G150				
			V4.7 S	P1 (All v	ersions	s),				
			SINAM	IICS G15	50 V4.8	(All				
			versio	ns < V4.	8 HF6),	-				
			SINAM	IICS G15	50 V5.1	(All				
			versio	ns), SIN	AMICS (G150				
			V5.1 S	P1 (All v	ersions	s < V5.1				
			SP1 HI	F4), SIN	AMICS S	5120				
			V4.6 (A	All versi	ons),					
			_	IICS S12	-	(All				
				ns), SIN		-				
				P1 (All v						
				IICS S12						
				ns < V4.		`				
				IICS S12	-					
				ns), SIN		•				
				P1 (All v						
				F4), SIN						
				All versi		- -				
			`	IICS S15	· ·	(All				
				ns), SIN		•				
				P1 (All v						
				IICS S15						
			versions < V4.8 HF6),							
				IICS S15	,					
CV Scoring Scale	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Type	pe(s): CSRF- Cross	Site Rea	uest Forg	ery; Dir. T	rav Dire	ctory Trav	ersal: +In	fo- Gain Ir	nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			V5.1 S SP1 H V5.1 (SINAM (All ve Manag SITOF version (All ve webse device vulne to a de condi cause situat restar the aff securi be exp with r affecte explore syster user in could to con the de advise public	F1 (All F4), SIN All vers MICS S2 ersions) ger (All PSU86 ons), SIT ersions) erver of es contarability enial-oftion. An a denialion which of the fected dity vulne oloited betwork ed system it ation ring privile it ation ring privile it at the inpromise exploit exploit ity vulne of the fected dity vulne oloited betwork ed system it at the inpromise exploit ity vulne of the fected dity vulne of the inpromise exploit ity vulne of the i	10 V5.11 Versions OO (All OP UPS TIM 15 The the affectins a that may service attacker cof-serv ch leads webserv evice. The erability by an att access t ms. Succe equires eges and on. An a vulnera	s < V5.1 S210 SP1 S), 1600 31 IRC cted r lead r may rice to a rer of ne could acker to the cessful no no ttacker bility bility of e of no this				
			CVE I	D : CVE-	2019-6	568				
simatic_cp443	8-1_firmware									
Improper Input	17-04-2019	5	A vulnerability has been identified in CP1604 (All						O-SIE-	-SIMA-
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 Typ	e(s): CSRF- Cross Denial of Service	_	_	-		_				n; DoS-

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIII	PC ID
Validation			versio	ons), CP1	L616 (Al	1			01051	9/420
				ns), SIA	•					,
				ersions)						
			_	3-1 Adva						
			versio	ns), SIM	IATIC CI	P443-1				
				ersions)						
			`	3-1 Adva						
				ns), SIM	_					
			OPC U	JA (All v	ersions)	,				
				TIC ET 2	_					
			Contr	oller CP	U 1515S	P PC				
			(All v	ersions •	< V2.1.6),				
			`	TIC ET 2	-					
				oller CP		-				
				ersions)						
			`	ort Outd						
				All versio						
			`	Comfort						
				ersions)						
			-	Mobile P						
				00, KTP						
				TP900F	•					
				TIC IPC 1	-	-				
				ersions)	_					
			`	1-EIP (A						
				TIC RF1		110),				
				ons), SIM	-	F186C				
				ersions)						
			`	8C (All v						
				TIC RF6		,				
				ns), SIM	•	7-1500				
				amily (A						
				TIC S7-1						
				oller (Al						
				TIC S7-3		-				
				ersions «		•				
			`	TIC S7-4						
				d below	•					
				u below TIC S7-4	-	-				
CV Scoring Scal	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			(incl.	F) (All v	ersions)	,				
			SIMA'	ΓIC S7-P	LCSIM					
			Advar	nced (All	version	ıs),				
			SIMA'	TIC Tele	service					
			Adapt	ter IE Ad	vanced	(All				
			versio	ns), SIM	IATIC					
			Teles	ervice A	dapter I	E Basic				
			(All v	ersions),	SIMAT	IC				
			Teles	ervice A	dapter II	Е				
			Stand	ard (All	version	s),				
			SIMA'	TIC Win	AC RTX	2010				
			(All v	ersions),	SIMAT	IC				
			WinC	C Runtin	ne Adva	nced				
			(All v	ersions),	SIMOC	ODE				
			pro V	EIP (All	version	s),				
			SIMO	CODE pr	o V PN (All				
			versio	ns), SIN	AMICS (G130				
				All versi						
			1	MICS G1:		(All				
				ns), SIN		•				
				SP1 (All						
				MICS G1:						
				ns < V4.		•				
				MICS G1:	-					
				ns), SIN		•				
				SP1 (All						
				F4), SIN						
				All versi						
			1	MICS G1		(All				
				ns), SIN		•				
				5P1 (All [,]						
				MICS G1:		· .				
				ons < V4.		•				
				MICS G1:	,					
				ons), SIN		•				
				SP1 (All						
				F4), SIN						
				All versi		7140				
			1	MICS S12		(All				
CV Scoring Scale	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross					ctory Trav		fo- Gain In		

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE	ID	Pat	tch	NCIII	PC ID
			versions), SI	NAMICS S	120				
			V4.7 SP1 (All	versions),				
			SINAMICS S1	20 V4.8 (All				
			versions < V	4.8 HF6),					
			SINAMICS S1	20 V5.1 (All				
			versions), SI	NAMICS S	120				
			V5.1 SP1 (All	versions	< V5.1				
			SP1 HF4), SI	NAMICS S	150				
			V4.6 (All ver	sions),					
			SINAMICS S1	50 V4.7 (All				
			versions), SI	NAMICS S	150				
			V4.7 SP1 (Al)	versions),				
			SINAMICS S1						
			versions < V	•					
			SINAMICS S1	•	All				
			versions), SI	•					
			V5.1 SP1 (All						
			SP1 HF4), SI						
			V5.1 (All ver						
			SINAMICS S2	-	SP1				
			(All versions						
			Manager (All	•).				
			SITOP PSU86		,,				
			versions), SI'	-	600				
			(All versions						
			(All versions		011110				
			webserver o	-	ted				
			devices cont		tou				
			vulnerability		lead				
			to a denial-o	-	icau				
			condition. Ar		may				
			cause a denia		•				
			situation wh						
			restart of the						
			the affected						
			security vuln	-					
			be exploited with networ	•					
			affected syst						
CV Scoring Scale	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross					_			

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
			syster user i could to cor the de advise public secur know	evice. At ory publ c exploit ity vulne n. D : CVE -	eges and on. An a vulnera ee availa the time ication of erability	no ttacker bility bility of e of no this was				
simatic_et_20	0_sp_open_co	ontrolle					1		<u>, </u>	
Improper Input Validation	17-04-2019	5	identiversic versic (All versic (All versic (All versic OPC USIMA' Contraction (All versic	nerability fied in Cons), CP1 ons), SIA ersions), 3-1 Adva ons), SIM ersions), 3-1 Adva ons), SIM IA (All versions), ort CET 2 coller CP ersions All versions) ort Outd All versions) fort Outd Comfort ersions) fort P2 OO, KTP2 TIC IPC I ersions)	EP1604 (All MTIC RILL AND CALL	[All 1 1 1 1 1 1 1 1 1	N/A			-SIMA- 19/421
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
<u> </u>	pe(s): CSRF- Cros	s Site Req	uest For	gery; Dir. 1	rav Dire	ctory Tray	ersal; +In	fo- Gain I	nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	D	escriptio	n & CVE	ID	Pa	tch	NCIII	PC ID
			RF181	-EIP (Al	l versio	ns),				
			SIMAT	IC RF18	32C (All					
			versio	ns), SIM	ATIC RI	F186C				
			(All ve	rsions),	SIMAT	C				
			RF188	C (All vo	ersions)	,				
			SIMAT	IC RF60	OR (All					
			versio	ns), SIM	ATIC S7	'-1500				
			CPU fa	mily (Al	l versio	ns),				
			SIMAT	IC S7-1	500 Sof	tware				
			Contro	ller (All	versio	ıs),				
			SIMAT	IC S7-3	00 CPU	family				
			(All ve	rsions <	V3.X.1	5),				
			SIMAT	IC S7-4	00 PN (i	ncl. F)				
			V6 and	l below	(All ver	sions),				
			SIMAT	IC S7-4	00 PN/I	OP V7				
			(incl. F) (All ve	ersions)	,				
			SIMAT	IC S7-P	LCSIM					
			Advan	ced (All	version	ıs),				
			SIMAT	IC Teles	ervice					
			Adapte	er IE Ad	vanced					
				ns), SIM						
			Telese	rvice Ad	lapter I	E Basic				
				rsions),	_					
			-	rvice Ac						
				rd (All	_					
				'IC Win		_				
			(All ve	rsions),	SIMAT	C				
			`	Runtin						
				rsions),						
			`	EIP (All						
			•	ODE pr		•				
				ns), SIN	1	•				
				All versi		1150				
			`	IICS G13		(A))				
				ns), SIN		•				
				113), 311v. P1 (All v						
				IICS G13						
				ns < V4.		(1111				
					о пгој, 80 V5.1	(All				
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
(CVSS) Vulnerability Ty										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIII	PC ID
			versions), SINAMICS G130				
			V5.1 SP1 (All versions < V5.	1			
			SP1 HF4), SINAMICS G150				
			V4.6 (All versions),				
			SINAMICS G150 V4.7 (All				
			versions), SINAMICS G150				
			V4.7 SP1 (All versions),				
			SINAMICS G150 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS G150 V5.1 (All				
			versions), SINAMICS G150				
			V5.1 SP1 (All versions < V5.	1			
			SP1 HF4), SINAMICS S120				
			V4.6 (All versions),				
			SINAMICS S120 V4.7 (All				
			versions), SINAMICS S120				
			V4.7 SP1 (All versions),				
			SINAMICS S120 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S120 V5.1 (All				
			versions), SINAMICS S120				
			V5.1 SP1 (All versions < V5.	1			
			SP1 HF4), SINAMICS S150	1			
			V4.6 (All versions),				
			SINAMICS S150 V4.7 (All				
			`				
			versions), SINAMICS S150				
			V4.7 SP1 (All versions),				
			SINAMICS S150 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S150 V5.1 (All				
			versions), SINAMICS S150				
			V5.1 SP1 (All versions < V5.	1			
			SP1 HF4), SINAMICS S210				
			V5.1 (All versions),				
			SINAMICS S210 V5.1 SP1				
	(All versions), SITOP Manager (All versions), SITOP PSU8600 (All						
			versions), SITOP UPS1600				
CV Scoring Sca	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1	1.2	3 7 4 3 3-0	0 /	, 0	3 3	J-10

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			(All von websed devices vulne to a decondition of the after security with a se	ersions) erver of es conta rability enial-of- tion. An a denial ion whice fected d ity vulne ploited b network ed syste itation r n privile use the npromis evice. At ory publ c exploit ity vulne ity vulne n.	the affeo ins a that may	ted vilead vilead vice to a ver of ne could acker o the cessful no no ttacker bility bility of e of no this was				
simatic_hmi_o	comiort_outa	oor_pai	•				I			
Improper Input Validation	17-04-2019	5	identi versic (All ve CP343 versic (All ve CP443 versic	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 Advanced (All versions), SIMATIC CP443-1 OPC UA (All versions),			N/A		O-SIE- 01051	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)										

Vulnerability Type(s)	Publish Date	cvss	Description	& CVE ID	Pat	ch	NCIII	PCID
			SIMATIC ET 20	0 SP Open				
			Controller CPU	1515SP PC				
			(All versions <	V2.1.6),				
			SIMATIC ET 20	0 SP Open				
			Controller CPU	1515SP PC2				
			(All versions), S	SIMATIC HMI				
			Comfort Outdo	or Panels 7" &				
			15" (All version	ıs), SIMATIC				
			HMI Comfort Pa	anels 4" - 22"				
			(All versions), S	SIMATIC HMI				
			KTP Mobile Par	nels KTP400F,				
			KTP700, KTP70	00F, KTP900				
			und KTP900F (All versions),				
			SIMATIC IPC Di	agMonitor				
			(All versions), S	SIMATIC				
			RF181-EIP (All	versions),				
			SIMATIC RF182	2C (All				
			versions), SIMA	TIC RF186C				
			(All versions), S	SIMATIC				
			RF188C (All ve	rsions),				
			SIMATIC RF600	-				
			versions), SIMA	TIC S7-1500				
			CPU family (All					
			SIMATIC S7-15	=				
			Controller (All	versions).				
			SIMATIC S7-30					
			(All versions <					
			SIMATIC S7-40	•				
			V6 and below (,				
			SIMATIC S7-40					
			(incl. F) (All ver	,				
			SIMATIC S7-PL	J .				
			Advanced (All v					
			SIMATIC Telese	•				
			Adapter IE Adv					
			versions), SIMA	•				
			Teleservice Ada					
			(All versions), S	_				
			Teleservice Adapter IE					
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-1
(CVSS)	0-1	1 2	2-3 3-4	7 3 3-0	0-7	7-0	0-3	5-1

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Par	tch	NCIII	PC ID
			Standard (All versions),				
			SIMATIC WinAC RTX 2010	0			
			(All versions), SIMATIC				
			WinCC Runtime Advanced	ŀ			
			(All versions), SIMOCODE				
			pro V EIP (All versions),				
			SIMOCODE pro V PN (All				
			versions), SINAMICS G130)			
			V4.6 (All versions),				
			SINAMICS G130 V4.7 (All				
			versions), SINAMICS G130)			
			V4.7 SP1 (All versions),				
			SINAMICS G130 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS G130 V5.1 (All				
			versions), SINAMICS G130)			
			V5.1 SP1 (All versions < V	5.1			
			SP1 HF4), SINAMICS G150)			
			V4.6 (All versions),				
			SINAMICS G150 V4.7 (All				
			versions), SINAMICS G150)			
			V4.7 SP1 (All versions),				
			SINAMICS G150 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS G150 V5.1 (All				
			versions), SINAMICS G150)			
			V5.1 SP1 (All versions < V				
			SP1 HF4), SINAMICS S120				
			V4.6 (All versions),				
			SINAMICS S120 V4.7 (All				
			versions), SINAMICS S120)			
			V4.7 SP1 (All versions),				
			SINAMICS S120 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S120 V5.1 (All				
			versions), SINAMICS S120)			
			V5.1 SP1 (All versions < V				
			SP1 HF4), SINAMICS S150				
			V4.6 (All versions),	,			
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-	-6 6-7	7-8	8-9	9-10
(CVSS)	V 1		3 , 13	0,	, 5	- 5 5	J 1

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pato	ch	NCIII	PCID
			SINAMICS S150 V4.7 (All				
			versions), SINAMICS S150				
			V4.7 SP1 (All versions),				
			SINAMICS S150 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S150 V5.1 (All				
			versions), SINAMICS S150				
			V5.1 SP1 (All versions < V5	5.1			
			SP1 HF4), SINAMICS S210				
			V5.1 (All versions),				
			SINAMICS S210 V5.1 SP1				
			(All versions), SITOP				
			Manager (All versions),				
			SITOP PSU8600 (All				
			versions), SITOP UPS1600				
			(All versions), TIM 1531 IF	RC.			
			(All versions). The				
			webserver of the affected				
			devices contains a				
			vulnerability that may lead				
			to a denial-of-service	`			
			condition. An attacker may				
			cause a denial-of-service				
			situation which leads to a				
			restart of the webserver of				
			the affected device. The				
			security vulnerability could	1			
			•				
			be exploited by an attacker with network access to the				
			affected systems. Successfu	ll			
			exploitation requires no				
			system privileges and no				
			user interaction. An attack				
			could use the vulnerability				
			to compromise availability	of			
			the device. At the time of				
			advisory publication no				
			public exploitation of this				
			security vulnerability was				
CV Scoring Sca	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1	1.2	3 7 7 3 3 6	, ,	, 0	3 3	J 1

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCI	IPC ID
			know	n.						
			CVE I	D : CVE-	2019-6	568				
simatic_hmi_o	comfort_pane	ls_firm	ware							
Improper Input Validation	17-04-2019	5	identi versic versic (All versic (All versic (All versic OPC U SIMA' Contr (All versic Comfe 15" (A HMI C (All versic	nerabilite fied in Cons), CP2 ons), SIA ersions), SIM ersions), SIM ersions), SIM (All vorsions), SIM (All versions) ort Outdot (All versions) ort O	EP1604 (ALC) EP1604 (ALC) EP1606 (ALC) EP160	All fragrammer and fr	N/A			-SIMA- 19/423
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
<u> </u>	pe(s): CSRF- Cross	Site Req	uest For	erv: Dir. 1	rav Dire	ctory Trav	ersal; +In	fo- Gain I	nformatio	n: DoS-

Vulnerability Type(s)	Publish Date	cvss	Description 8	& CVE ID	Pat	tch	NCIII	PC ID
			Controller (All v	ersions),				
			SIMATIC S7-300	CPU family				
			(All versions < V	3.X.16),				
			SIMATIC S7-400	PN (incl. F)				
			V6 and below (A	ll versions),				
			SIMATIC S7-400	PN/DP V7				
			(incl. F) (All vers	ions),				
			SIMATIC S7-PLC	SIM				
			Advanced (All ve	ersions),				
			SIMATIC Teleser	vice				
			Adapter IE Adva	nced (All				
			versions), SIMAT	CIC				
			Teleservice Adap	ter IE Basic				
			(All versions), SI					
			Teleservice Ada					
			Standard (All ve	rsions),				
			SIMATIC WinAC	-				
			(All versions), SI					
			WinCC Runtime					
			(All versions), SI	MOCODE				
			pro V EIP (All ve					
			SIMOCODE pro V	,				
			versions), SINAM	`				
			V4.6 (All version					
			SINAMICS G130	,				
			versions), SINAM	`				
			V4.7 SP1 (All ver					
			SINAMICS G130	· ·				
			versions < V4.8 I	`				
			SINAMICS G130	-				
			versions), SINAM	`				
			-					
			V5.1 SP1 (All ver					
			SP1 HF4), SINAN					
			V4.6 (All version	-				
			SINAMICS G150	`				
			versions), SINAN					
			V4.7 SP1 (All ver					
			SINAMICS G150 versions < V4.8 I	`				
CV Scoring Scal	e	4.0		-	6.7	- 0		
(CVSS)	0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	1	NCIIF	PC ID
			SINAMICS G150 V5.1 (All				
			versions), SINAMICS G150				
			V5.1 SP1 (All versions < V5.	1			
			SP1 HF4), SINAMICS S120				
			V4.6 (All versions),				
			SINAMICS S120 V4.7 (All				
			versions), SINAMICS S120				
			V4.7 SP1 (All versions),				
			SINAMICS S120 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S120 V5.1 (All				
			versions), SINAMICS \$120				
			V5.1 SP1 (All versions < V5.	1			
			SP1 HF4), SINAMICS S150				
			V4.6 (All versions),				
			SINAMICS S150 V4.7 (All				
			versions), SINAMICS S150				
			V4.7 SP1 (All versions),				
			SINAMICS S150 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S150 V5.1 (All				
			versions), SINAMICS S150				
			V5.1 SP1 (All versions < V5.	1			
			SP1 HF4), SINAMICS S210	1			
			V5.1 (All versions),				
			SINAMICS S210 V5.1 SP1				
			(All versions), SITOP				
			Manager (All versions),				
			SITOP PSU8600 (All				
			versions), SITOP UPS1600	,			
			(All versions), TIM 1531 IR(<i>:</i>			
			(All versions). The				
			webserver of the affected				
			devices contains a				
			vulnerability that may lead				
			to a denial-of-service				
			condition. An attacker may				
			cause a denial-of-service				
			situation which leads to a				
CV Scoring Sca	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-0	0-7	7-0	0-3	5-1

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	า	NCIII	PC ID
			restart of the webserver of the affected device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.				
simatic hmi l	ktp mobile pa	nels k	tp400f firmware				
Improper Input Validation	nput 17-04-2019 5		A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2 (All versions), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions), SIMATIC HMI Comfort Panels 4" - 22"	N/A		0-SIE- 01051	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
		_	uest Forgery; Dir. Trav Directory Trav oss Site Scripting; Sql- SQL Injection; N 296			formatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	D	escriptio	n & CVE	ID	Pa	tch	NCIII	PC ID
			(All ve	rsions),	SIMAT	C HMI				
			KTP M	obile Pa	nels KT	'P400F,				
			KTP70	0, KTP7	'00F, KT	ГР900				
			und K7	ГР900F	(All ver	sions),				
			SIMAT	IC IPC D	DiagMor	itor				
			(All ve	rsions),	SIMAT	(C				
			RF181	-EIP (Al	l versio	ns),				
			SIMAT	IC RF18	32C (All					
			versio	ns), SIM	ATIC RI	F186C				
			(All ve	rsions),	SIMAT	C				
			RF188	C (All ve	ersions)	,				
			SIMAT	IC RF60	OR (All					
			versio	ns), SIM	ATIC S7	'-1500				
			CPU fa	mily (Al	l versio	ns),				
			SIMAT	IC S7-1	500 Sof	tware				
			Contro	ller (All	versio	1s),				
			SIMAT	IC S7-3	00 CPU	family				
			(All ve	rsions <	V3.X.1	6),				
			SIMAT	IC S7-4	00 PN (i	ncl. F)				
			V6 and	below	(All ver	sions),				
			SIMAT	IC S7-4	00 PN/I	OP V7				
			(incl. F	(All ve	ersions)	,				
			SIMAT	IC S7-P	LCSIM					
			Advan	ced (All	version	ıs),				
			SIMAT	IC Teles	service					
			Adapte	er IE Ad	vanced	(All				
			versio	ns), SIM	ATIC					
			Telese	rvice Ad	lapter I	E Basic				
			(All ve	rsions),	SIMAT	IC .				
			Telese	rvice Ad	lapter I	Е				
			Standa	rd (All	version	s),				
			SIMAT	IC Win	AC RTX	2010				
			(All ve	rsions),	SIMAT	IC .				
			WinCC	Runtin	ie Adva	nced				
			(All ve	rsions),	SIMOC	ODE				
			pro V I	EIP (All	version	s),				
			SIMOC	ODE pr	o V PN (All				
			versio	ns), SIN	AMICS (G130				
			V4.6 (A	All versi	ons),					
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross									

Vulnerability Type(s)	Publish Date	cvss	Description	& CVE ID	Pat	tch	NCIII	PC ID
			SINAMICS G130) V4.7 (All				
			versions), SINA	MICS G130				
			V4.7 SP1 (All ve	ersions),				
			SINAMICS G130) V4.8 (All				
			versions < V4.8	HF6),				
			SINAMICS G130) V5.1 (All				
			versions), SINA	MICS G130				
			V5.1 SP1 (All ve	ersions < V5.1				
			SP1 HF4), SINA	MICS G150				
			V4.6 (All versio	ns),				
			SINAMICS G150) V4.7 (All				
			versions), SINA	MICS G150				
			V4.7 SP1 (All ve					
			SINAMICS G150	-				
			versions < V4.8	•				
			SINAMICS G150					
			versions), SINA	•				
			V5.1 SP1 (All ve					
			SP1 HF4), SINA					
			V4.6 (All versio					
			SINAMICS S120	-				
			versions), SINA	•				
			V4.7 SP1 (All ve					
			SINAMICS S120	-				
			versions < V4.8	-				
			SINAMICS S120	<i>3.</i>				
			versions), SINA	•				
			V5.1 SP1 (All ve					
			SP1 HF4), SINA					
			V4.6 (All versio					
			`	.				
			SINAMICS S150	•				
			versions), SINA					
			V4.7 SP1 (All ve	•				
			SINAMICS S150	•				
			versions < V4.8	•				
			SINAMICS S150	-				
			versions), SINA					
			V5.1 SP1 (All ve					
			SP1 HF4), SINA	MICS 5210				
CV Scoring Sca	0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)	rpe(s): CSRF- Cross	Cita Dan						

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			SINAN (All ve Mana) SITOF version (All ve Webse device vulne to a decondification of the affect explored system user in could to continue to a device with market explored system user in could to continue decondification of the de	evice. At ory publ c exploit ity vulne	the the affections a service attacker access the eads access to the eads access to the ead access to t	s), 1600 31 IRC cted y lead r may vice to a ver of he could acker to the cessful no no ttacker bility bility of e of no this was				
simatic_hmi_k	tn mohile na	nels k								
	r = ···································			nerabilit		en				
Improper Input Validation	17-04-2019	5	identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC			(All ll F185C	N/A			-SIMA- 19/425
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 Typ	pe(s): CSRF- Cross Denial of Service	_				-			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIII	PC ID
			CP343-1 Advanced (All				
			versions), SIMATIC CP443-	1			
			(All versions), SIMATIC				
			CP443-1 Advanced (All				
			versions), SIMATIC CP443-	1			
			OPC UA (All versions),				
			SIMATIC ET 200 SP Open				
			Controller CPU 1515SP PC				
			(All versions < V2.1.6),				
			SIMATIC ET 200 SP Open				
			Controller CPU 1515SP PC	2			
			(All versions), SIMATIC HM	1I			
			Comfort Outdoor Panels 7"	&			
			15" (All versions), SIMATIO				
			HMI Comfort Panels 4" - 22	2"			
			(All versions), SIMATIC HM	1I			
			KTP Mobile Panels KTP400)F,			
			KTP700, KTP700F, KTP900)			
			und KTP900F (All versions	3),			
			SIMATIC IPC DiagMonitor				
			(All versions), SIMATIC				
			RF181-EIP (All versions),				
			SIMATIC RF182C (All				
			versions), SIMATIC RF1860	C			
			(All versions), SIMATIC				
			RF188C (All versions),				
			SIMATIC RF600R (All				
			versions), SIMATIC S7-150	0			
			CPU family (All versions),				
			SIMATIC S7-1500 Software	2			
			Controller (All versions),				
			SIMATIC S7-300 CPU famil	v			
			(All versions < V3.X.16),				
			SIMATIC S7-400 PN (incl. F	7)			
			V6 and below (All versions	_			
			SIMATIC S7-400 PN/DP V7	-			
			(incl. F) (All versions),				
			SIMATIC S7-PLCSIM				
			Advanced (All versions),				
CV Scoring Scal	e e						
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	De	escription & CV	E ID	Pa	tch	NCIII	PC ID
			SIMATI	C Teleservice	<u> </u>				
			Adapte	r IE Advance	l (All				
			version	s), SIMATIC					
			Teleser	vice Adapter	IE Basic				
				rsions), SIMA'					
			`	vice Adapter					
				rd (All versio					
			SIMATI	C WinAC RTX	2010				
			(All ver	rsions), SIMA'	ГІС				
			`	Runtime Adv					
			(All ver	sions), SIMO	CODE				
			_	IP (All versio					
			•	DDE pro V PN	-				
				s), SINAMICS	-				
				ll versions),	G100				
			`	ICS G130 V4.7	7 (All				
				s), SINAMICS	•				
				1 (All version					
				ICS G130 V4.8					
				s < V4.8 HF6	•				
				ICS G130 V5.1					
				ics d130 v3 is), SINAMICS	•				
				13), Silvamics 1 (All version					
				4), SINAMICS					
					G130				
			-	ll versions),	7 (
				ICS G150 V4.7					
				s), SINAMICS					
				1 (All version					
				ICS G150 V4.8	•				
				s < V4.8 HF6					
				ICS G150 V5.2					
				s), SINAMICS					
				1 (All version					
				4), SINAMICS	S120				
			V4.6 (A	ll versions),					
				ICS S120 V4.7	•				
				s), SINAMICS					
			V4.7 SP1 (All versions),						
			SINAM						
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE	ID Pa	tch	NCIII	PC ID
			versions < V4.8 HF6),				
			SINAMICS S120 V5.1	(All			
			versions), SINAMICS S	5120			
			V5.1 SP1 (All versions	s < V5.1			
			SP1 HF4), SINAMICS S	5150			
			V4.6 (All versions),				
			SINAMICS S150 V4.7	All			
			versions), SINAMICS S	-			
			V4.7 SP1 (All versions				
			SINAMICS S150 V4.8	*			
			versions < V4.8 HF6),				
			SINAMICS S150 V5.1	(All			
			versions), SINAMICS S	`			
			V5.1 SP1 (All versions				
			SP1 HF4), SINAMICS S				
			V5.1 (All versions),	5210			
			SINAMICS S210 V5.1	SD1			
			(All versions), SITOP	51 1			
			•				
			Manager (All versions), 			
			SITOP PSU8600 (All	1600			
			versions), SITOP UPS:				
			(All versions), TIM 15	31 IKC			
			(All versions). The	. 1			
			webserver of the affec	cted			
			devices contains a				
			vulnerability that may	7 lead			
			to a denial-of-service				
			condition. An attacker	·			
			cause a denial-of-serv				
			situation which leads				
			restart of the webserv	er of			
			the affected device. Th	ne			
			security vulnerability	could			
			be exploited by an att	acker			
			with network access t	o the			
			affected systems. Succ	cessful			
			exploitation requires	no			
			system privileges and				
			user interaction. An a				
CV Scoring Sca	le 0.1	1.2	22 24 45	5.6	7.0	9.0	0.4
(CVSS)	0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-1

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID Patch NCIIPO				
			could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6568				
simatic_teles	_ ervice_adapte	r_ie_st	andard_firmware				
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIAMTIC RF185C (CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2 (All versions), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions), SIMATIC HMI Comfort Panels 4" - 22" (All versions), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 und KTP900F (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF186C	N/A		O-SIE-5 01051	
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CVE	ID	Pa	tch	NCIII	PC ID
			(All version	s), SIMAT	C				
			RF188C (Al	versions	,				
			SIMATIC RE	600R (All					
			versions), S	IMATIC S7	'-1500				
			CPU family						
			SIMATIC S7	•					
			Controller (
			SIMATIC S7		-				
			(All version		-				
			SIMATIC S7		-				
			V6 and belo	•	,				
			SIMATIC S7	•	٠.				
				•					
			(incl. F) (All	_	,				
			SIMATIC S7		-3				
			Advanced (A		ıSJ,				
			SIMATIC Te		C A 11				
			Adapter IE		(All				
			versions), S						
			Teleservice	_					
			(All version	-					
			Teleservice	Adapter I	Ε				
			Standard (A	ll version	s),				
			SIMATIC W	inAC RTX	2010				
			(All version	s), SIMAT	C				
			WinCC Run	time Adva	nced				
			(All version	s), SIMOC	ODE				
			pro V EIP (A	All version	s),				
			SIMOCODE	pro V PN (All				
			versions), S	INAMICS (G130				
			V4.6 (All ve						
			SINAMICS C	-	(All				
			versions), S		`				
			V4.7 SP1 (A						
			SINAMICS O						
					ניזוו				
			versions < \	•	C A 11				
			SINAMICS (`				
			versions), S						
			V5.1 SP1 (A SP1 HF4), S						
CV Scoring Sca			3F 1 11F4J, 3	IIVAIVII (3 (1120				
(CVSS)	0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-1

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pa	tch	NCIII	PC ID
			V4.6 (All versions),				
			SINAMICS G150 V4.7 (A	.11			
			versions), SINAMICS G1	.50			
			V4.7 SP1 (All versions),				
			SINAMICS G150 V4.8 (A	.11			
			versions < V4.8 HF6),				
			SINAMICS G150 V5.1 (A	.11			
			versions), SINAMICS G1	50			
			V5.1 SP1 (All versions <	: V5.1			
			SP1 HF4), SINAMICS S1	20			
			V4.6 (All versions),				
			SINAMICS S120 V4.7 (A	11			
			versions), SINAMICS S1				
			V4.7 SP1 (All versions),				
			SINAMICS S120 V4.8 (A				
			versions < V4.8 HF6),				
			SINAMICS S120 V5.1 (A	11			
			versions), SINAMICS S1				
			V5.1 SP1 (All versions <				
			SP1 HF4), SINAMICS S1				
			V4.6 (All versions),				
			SINAMICS S150 V4.7 (A	11			
			versions), SINAMICS S1				
			V4.7 SP1 (All versions),				
			SINAMICS S150 V4.8 (A				
			versions < V4.8 HF6),	"			
			SINAMICS S150 V5.1 (A	11			
			,				
			versions), SINAMICS S1				
			V5.1 SP1 (All versions <				
			SP1 HF4), SINAMICS S2	10			
			V5.1 (All versions),				
			SINAMICS S210 V5.1 SP	'1			
			(All versions), SITOP				
			Manager (All versions),				
			SITOP PSU8600 (All				
			versions), SITOP UPS16				
			(All versions), TIM 1532	1 IRC			
			(All versions). The				
			webserver of the affecte	ed			
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-1
(CVSS)	- 01		37 43	0.7	, 0	3 3	J 1

Vulnerability Type(s)	Publish Date	cvss	1	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			vulne to a d condi cause situat restar the af secur be exp with r affect explo syster user i could to cor the de advise public secur know	evice. At ory publ e exploit ity vulne	that may service attacked attacked of service. The rability of an att access to equires eges and on. An avulnera the time attaction of erability	may rice to a ver of ne could acker to the cessful no no ttacker bility bility of e of no this was				
simatic_winac	_rtx_2010_fi	rmware	e							
Improper Input Validation	17-04-2019	5	identi versic (All versic (All versic (All versic (P44: versic OPC U SIMA' Contr	nerabilit fied in C ons), CP1 ons), SIA ersions) 3-1 Adva ons), SIM JA (All v TIC ET 2 oller CP	P1604 (Al Al A	[All l l l l l l l l l l l l l l l l l l	N/A			-SIMA- .9/427
CV Scoring Scale							6-7			

Vulnerability Type(s)	Publish Date	cvss	Descriptio	n & CVE ID	Pa	tch	NCIII	PC ID
			SIMATIC ET 20	00 SP Open				
			Controller CPU	J 1515SP PC2				
			(All versions),	SIMATIC HMI				
			Comfort Outdo	or Panels 7" 8	ı			
			15" (All versio	ns), SIMATIC				
			HMI Comfort F					
			(All versions),	SIMATIC HMI				
			KTP Mobile Pa	nels KTP400F	,			
			KTP700, KTP7	00F, KTP900				
			und KTP900F	(All versions),				
			SIMATIC IPC D	iagMonitor				
			(All versions),	SIMATIC				
			RF181-EIP (Al					
			SIMATIC RF18	-				
			versions), SIM.	-				
			(All versions),					
			RF188C (All ve					
			SIMATIC RF60					
			versions), SIM	•				
			CPU family (Al					
			SIMATIC S7-15	•				
			Controller (All					
			SIMATIC S7-30	•				
			(All versions <	-				
			`	•				
			SIMATIC S7-40					
			V6 and below	,				
			SIMATIC S7-4(•				
			(incl. F) (All ve	J .				
			SIMATIC S7-PI					
			Advanced (All	-				
			SIMATIC Teles					
			Adapter IE Adv	-				
			versions), SIM					
			Teleservice Ad	-				
			(All versions),					
			Teleservice Ad	-				
			Standard (All v	versions),				
			SIMATIC WinA					
			(All versions),	SIMATIC				
CV Scoring Sca	e 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)	0-1	1-2	2-3 3-4	4-5	0-7	7-0	0-3	3-10

Vulnerability Type(s)	Publish Date	cvss	Descr	iption & CVE	ID	Pa	tch	NCIII	PC ID
			WinCC Ru	ntime Adva	nced				
			(All versio	ns), SIMOC	ODE				
			pro V EIP	(All version	s),				
			SIMOCOD	E pro V PN (All				
			versions),	SINAMICS (G130				
			V4.6 (All v	ersions),					
			SINAMICS	G130 V4.7	(All				
			versions),	SINAMICS (G130				
			V4.7 SP1 (All versions	s),				
			SINAMICS	G130 V4.8	(All				
			versions <	V4.8 HF6),					
			SINAMICS	G130 V5.1	(All				
			versions),	SINAMICS (G130				
			V5.1 SP1 (All versions	< V5.1				
			SP1 HF4),	SINAMICS (G150				
			V4.6 (All v	ersions),					
			SINAMICS	G150 V4.7	(All				
			versions),	SINAMICS (G150				
			V4.7 SP1 (All versions	s),				
			SINAMICS	G150 V4.8	(All				
			versions <	V4.8 HF6),					
			SINAMICS	G150 V5.1	(All				
			versions),	SINAMICS (G150				
			-	All versions					
			`	SINAMICS S					
			V4.6 (All v						
			`	S120 V4.7	All				
				SINAMICS S	•				
			-	All versions					
			`	S120 V4.8					
				V4.8 HF6),					
				S120 V5.1	All				
				SINAMICS S	•				
			-	All versions					
			`	SINAMICS S					
			V4.6 (All v		,130				
			-	S150 V4.7 (A 11				
				SINAMICS S	•				
			-	All versions					
CV Scoring Sca	le 0-1	1-2	2-3 3-	4 4-5	5-6	6-7	7-8	8-9	9-1
(CVSS) Vulnerability Ty									

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SINAMICS S150 V4.8 (All		
			versions < V4.8 HF6),		
			SINAMICS S150 V5.1 (All		
			versions), SINAMICS S150		
			V5.1 SP1 (All versions < V5.1		
			SP1 HF4), SINAMICS S210		
			V5.1 (All versions),		
			SINAMICS S210 V5.1 SP1		
			(All versions), SITOP		
			Manager (All versions),		
			SITOP PSU8600 (All		
			versions), SITOP UPS1600		
			(All versions), TIM 1531 IRC		
			(All versions). The		
			webserver of the affected		
			devices contains a		
			vulnerability that may lead		
			to a denial-of-service		
			condition. An attacker may		
			cause a denial-of-service		
			situation which leads to a		
			restart of the webserver of		
			the affected device. The		
			security vulnerability could		
			be exploited by an attacker		
			with network access to the		
			affected systems. Successful		
			exploitation requires no		
			system privileges and no		
			user interaction. An attacker		
			could use the vulnerability		
			to compromise availability of		
			the device. At the time of		
			advisory publication no		
			public exploitation of this		
			security vulnerability was		
			known.		
			CVE ID : CVE-2019-6568		

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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
simocode_pro	_v_eip_firmw	are			
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2 (All versions), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions), SIMATIC HMI Comfort Panels 4" - 22" (All versions), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 und KTP900F (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF188C (All versions), SIMATIC S7-1500 CPU family (All versions), SIMATIC S7-300 CPU family	N/A	O-SIE-SIMO- 010519/428

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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; Dos-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	De	escriptior	a & CVE	ID	Pa	tch	NCIII	PC ID
			(All ve	rsions <	V3.X.16	ó),				
			SIMAT	IC S7-40	0 PN (i	ncl. F)				
			V6 and	below (All ver	sions),				
			SIMAT	IC S7-40	0 PN/I)P V7				
			(incl. F) (All ve	rsions)					
			SIMAT	IC S7-PL	CSIM					
			Advano	ced (All v	version	s),				
			SIMAT	IC Telese	ervice					
			Adapte	r IE Adv	anced	(All				
			version	ns), SIM <i>A</i>	ATIC					
				rvice Ada		E Basic				
				rsions), S	_					
			-	rvice Ada						
				rd (All v	•					
				IC WinA		-				
			_	rsions), S	_					
			`	Runtim						
				rsions), S						
			-	EIP (All v						
			_	ODE pro						
				rs), SINA	•					
				all versio		1130				
			-	ICS G13	-	Δ11				
				is), SINA		-				
				15), 311VA P1 (All vo						
				ICS G13						
						AII				
				rs < V4.8	-	7 A 11				
				ICS G13		•				
				is), SINA						
				P1 (All v						
				(4), SINA		150				
			`	All versio						
				ICS G15		•				
				ıs), SINA						
				P1 (All v						
				ICS G15		All				
				ns < V4.8	-					
		SINAMICS G150 V5.1 (All								
			versior	ıs), SINA	MICS (150				
CV Scoring Scal	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty			23	3 4	, 3	30	3,	, 0	0 3	J 10

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CVE	ID	Pa	tch	NCIII	PC ID
			V5.1 SP1 (A)	l versions	< V5.1				
			SP1 HF4), SI						
			V4.6 (All vei						
			SINAMICS S	-	All				
			versions), Sl		•				
			V4.7 SP1 (A)						
			SINAMICS S						
			versions < V		•				
			SINAMICS S		All				
			versions), Sl		•				
			V5.1 SP1 (A)						
			SP1 HF4), SI						
			V4.6 (All vei		0				
			SINAMICS S	-	All				
			versions), Sl		•				
			V4.7 SP1 (A)						
			SINAMICS S		_				
			versions < V		2 111				
			SINAMICS S		Δll				
			versions), Sl		•				
			V5.1 SP1 (A)						
			SP1 HF4), SI						
			V5.1 (All ver		210				
			SINAMICS S	-	SD1				
			(All versions)1 1				
			Manager (Al	-	1				
			SITOP PSU8		بل				
			versions), Sl	•	600				
			7.						
			(All versions	-	31 IKC				
			(All versions	-					
			webserver o		tea				
			devices cont						
			vulnerability		lead				
			to a denial-c						
			condition. A		•				
			cause a deni						
			situation wh						
			restart of th						
			the affected	device. Tł	ie				
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-1
(CVSS)			2 3 4	7 3	3 0	5 ,	, 0		J 1

security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication of this security vulnerability was known. CVE ID: CVE-2019-6568 Simocode_pro_v_pn_firmware A vulnerability has been identified in CP1604 (All versions), SIMATIC (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443	Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
Simocode_pro_v_pn_firmware A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2 (All versions), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions), SIMATIC HMI Comfort Panels 4" - 22" (All versions), SIMATIC HMI				be explosive the deadvise public security know	ploited be networked system itation response in privile use the mpromise evice. At ory public exploit ity vulne n.	by an att access t ms. Succe equires eges and on. An a vulnera se availa the time ication of erability	acker to the cessful no no ttacker bility bility of e of no this was				
Improper Input Validation 17-04-2019 Validation 17-04-2019 Validation 17-04-2019 Validation 17-04-2019 Validation 17-04-2019 Validation 17-04-2019 Imput Validation 17-04-2019 V	simocode pro	y nn firmw	are	CVE I	D : CVE-	2019-6	568				
	Input	17-04-2019	5	identi versic (All versic (All versic (All versic (All versic OPC U SIMA' Contr (All versic (All versi	fied in Cons), CP2 ons), SIA ersions) 3-1 Adva ons), SIM ersions), SIM JA (All v TIC ET 2 oller CP ersions of TIC ET 2 oller CP ersions) ort Outd All versions)	EP1604 (All 1616 (All MTIC RI), SIMATE CION (ALL 1616 (A	(All ll F185C IC still P443-1 IC still PC ll PC	N/A			
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9	_	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	[Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			KTP7	00, KTP	700F, KT	ГР900				
			und K	TP900F	(All ver	sions),				
			SIMA	ΓIC IPC I	DiagMor	nitor				
			(All ve	ersions)	, SIMAT	IC				
			RF181	l-EIP (A	ll versio	ns),				
			SIMA	ΓIC RF1	32C (All					
			versio	ns), SIM	IATIC RI	F186C				
			(All ve	ersions)	, SIMAT	IC				
			RF188	BC (All v	ersions)),				
			SIMA	ΓIC RF6	OOR (All					
			versio	ns), SIM	IATIC S7	7-1500				
			CPU fa	amily (A	ll versio	ns),				
			SIMA	ΓIC S7-1	500 Sof	tware				
			Contr	oller (Al	l versioi	ns),				
			SIMA	ΓIC S7-3	00 CPU	family				
			(All ve	ersions	< V3.X.1	6),				
			SIMA	ΓIC S7-4	00 PN (i	incl. F)				
			V6 an	d below	(All ver	sions),				
			SIMA	ΓIC S7-4	00 PN/I	OP V7				
			(incl.	F) (All v	ersions)	,				
			SIMA	ΓIC S7-P	LCSIM					
				-	version	ıs),				
			SIMA	ΓIC Tele	service					
			_		vanced	(All				
				ns), SIM						
					dapter I					
			`		, SIMAT					
					dapter II					
				•	version	-				
					AC RTX					
			`	-	, SIMAT					
					ne Adva					
			`	-	, SIMOC					
			_	•	version	-				
				•	o V PN (•				
				-	AMICS (i130				
		V4.6 (All versions),								
					30 V4.7	•				
			versio	ns), SIN	AMICS (i130 ———			<u> </u>	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Tvi	pe(s): CSRF- Cross		uest Fore	ery: Dir. 1	rav Dire	ctory Trav	ersal: +In	fo- Gain Ir	nformatio	n: DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PCID
			V4.7 S	P1 (All	versions	;),				
			SINAN	AICS G1	30 V4.8	(All				
			versio	ns < V4	.8 HF6),					
			SINAN	AICS G1	30 V5.1	(All				
			versio	ns), SIN	AMICS (G130				
			V5.1 S	SP1 (All	versions	< V5.1				
			SP1 H	F4), SIN	AMICS (G150				
			V4.6 (All vers	ions),					
			SINAN	AICS G1	50 V4.7	(All				
			versio	ns), SIN	AMICS (G150				
			V4.7 S	P1 (All	versions	3),				
			SINAN	AICS G1	50 V4.8	(All				
			versio	ns < V4	.8 HF6),					
			SINAN	AICS G1	50 V5.1	(All				
			versio	ns), SIN	AMICS (G150				
			V5.1 S	SP1 (All	versions	< V5.1				
			SP1 H	F4), SIN	AMICS S	3120				
				All vers						
			SINAN	AICS S12	20 V4.7 (All				
			versio	ns), SIN	AMICS S	5120				
			V4.7 S	SP1 (All	versions	i),				
			SINAN	AICS S12	20 V4.8 (All				
					.8 HF6),					
					20 V5.1 (All				
					AMICS S	•				
			V5.1 S	P1 (All	versions	< V5.1				
				-	AMICS S					
				All vers						
			`		50 V4.7 (All				
					AMICS S	•				
					versions					
				•	50 V4.8 (-				
					.8 HF6),					
					-	All				
				SINAMICS S150 V5.1 (All versions) SINAMICS S150						
			versions), SINAMICS S150 V5.1 SP1 (All versions < V5.1							
	SP1 HF4), SINAMICS S210									
	V5.1 (All versions),									
			1		10113), 10 V5.1 S	SP1				
CV Scoring Sca	le le						1			
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

			Manage SITOF version (All version (All version (All version (All version vulner) to a decondification of the affector of the decondification of the decondificat	ersions) ger (All sersions) gersions) ersions) ersions) erver of es containability sersion. An a denial ion which ion which it of the sersion	versions 00 (All 0P UPS) TIM 15 The the affect ins a that may service attacker of-serv ch leads webserv evice. The trability y an attaces to equires eges and on. An act vulneral the time ication re ation of erability	ted ted lead lead may ice to a rer of ne could acker o the cessful no no ttacker bility bility of e of no this was				
sinamics_s150	_firmware									
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1			[All l F185C IC ll	N/A		0-SIE- 01051	-SINA- 19/430
CV Scoring Scale (CVSS) Vulnerability Typ	0-1	1-2 Site Req	2-3 uest Forg	3-4 gery; Dir. 1	4-5 rav Dire	5-6	6-7 ersal; +In	7-8 fo- Gain In	8-9	9-10 on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description &	CVE ID	Pat	tch	NCIII	PC ID	
			(All versions), SIM	1ATIC					
			CP443-1 Advance	d (All					
			versions), SIMATI	C CP443-1					
			OPC UA (All versi	ons),					
			SIMATIC ET 200 S	SP Open					
			Controller CPU 15	S15SP PC					
			(All versions < V2	.1.6),					
			SIMATIC ET 200 S	SP Open					
			Controller CPU 15	S15SP PC2					
			(All versions), SIN	IATIC HMI					
			Comfort Outdoor	Panels 7" &					
			15" (All versions)	, SIMATIC					
			HMI Comfort Pan	els 4" - 22"					
			(All versions), SIN	IATIC HMI					
			KTP Mobile Panel	s KTP400F,					
			KTP700, KTP7001	F, KTP900					
			und KTP900F (Al	versions),					
			SIMATIC IPC Diag	Monitor					
			(All versions), SIM	1ATIC					
			RF181-EIP (All ve	rsions),					
			SIMATIC RF182C	-					
			versions), SIMATI	-					
			(All versions), SIM						
			RF188C (All versi						
			SIMATIC RF600R	-					
			versions), SIMATI	•					
			CPU family (All ve						
			SIMATIC S7-1500	· .					
			Controller (All ve						
			SIMATIC S7-300 (-					
			(All versions < V3	-					
			SIMATIC S7-400 I	-					
			V6 and below (All	,					
			SIMATIC S7-400 I	,					
				,					
			(incl. F) (All versions), SIMATIC S7-PLCSIM						
Advanced (All versions) SIMATIC Teleservice				-					
			Adapter IE Advan						
CV Scoring Scal	<u> </u>		Thurpter IL Auvall	ccu (IIII					
(CVSS)	0-1	1-2	2-3 3-4 4	-5 5-6	6-7	7-8	8-9	9-10	

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE	ID	Pa	tch	NCIII	PC ID
			versions), SI	MATIC					
			Teleservice A	dapter I	E Basic				
			(All versions), SIMAT	C				
			Teleservice A	dapter I	Ξ				
			Standard (Al	l version:	s),				
			SIMATIC Wii	AC RTX	2010				
			(All versions), SIMAT	C				
			WinCC Runti	me Adva	nced				
			(All versions), SIMOC	ODE				
			pro V EIP (A	l version	s),				
			SIMOCODE p	ro V PN (All				
			versions), SI	NAMICS (G130				
			V4.6 (All ver						
			SINAMICS G	-	(All				
			versions), SI		•				
			V4.7 SP1 (Al						
			SINAMICS G		•				
			versions < V		(1.11				
			SINAMICS G	-	(A))				
			versions), SI		•				
			V5.1 SP1 (Al						
			SP1 HF4), SI						
			V4.6 (All ver		1130				
			SINAMICS G	-	(A))				
					-				
			versions), SI						
			V4.7 SP1 (Al		•				
			SINAMICS G		(AII				
			versions < V	-	C A 11				
			SINAMICS G		•				
			versions), SI						
			V5.1 SP1 (Al						
			SP1 HF4), SI		5120				
			V4.6 (All ver						
			SINAMICS S1		-				
			versions), SI						
			V4.7 SP1 (Al						
			SINAMICS S1	20 V4.8	All				
			versions < V	4.8 HF6),					
			SINAMICS S1	20 V5.1	[All				
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0-1	1-2	2-3 3-4	4-3	3-0	0-7	7-8	0-3	5-10

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			versio	ns), SIN	AMICS S	5120				
			V5.1 S	P1 (All	versions	s < V5.1				
			SP1 H	F4), SIN	AMICS S	S150				
			V4.6 (All vers	ions),					
			SINAN	AICS S1	50 V4.7	(All				
			versio	ns), SIN	AMICS S	S150				
			V4.7 S	P1 (All	versions	s),				
			SINAN	AICS S1	50 V4.8	(All				
			versio	ns < V4	.8 HF6),					
			SINAN	AICS S1	50 V5.1	(All				
			versio	ns), SIN	AMICS S	S150				
			V5.1 S	P1 (All	versions	s < V5.1				
			SP1 H	F4), SIN	AMICS S	5210				
			V5.1 (All vers	ions),					
			SINAN	AICS S2	10 V5.1	SP1				
			(All ve	ersions)	, SITOP					
			Mana	ger (All	versions	s),				
			SITOF	PSU86	00 (All					
			versio	ns), SIT	OP UPS:	1600				
			(All ve	ersions)	, TIM 15	31 IRC				
			(All ve	ersions)	. The					
			webse	erver of	the affe	cted				
			device	es conta	ins a					
			vulne	rability	that may	lead				
			to a d	enial-of	service					
			condi	tion. An	attackei	may				
			cause	a denia	l-of-serv	ice				
			situat	ion whi	ch leads	to a				
			restar	t of the	webserv	er of				
			the af	fected d	evice. Tl	ne				
			securi	ty vulne	erability	could				
			be exp	oloited b	y an att	acker				
			1		access t					
			affect	ed syste	ms. Succ	cessful				
				•	equires					
			_		eges and					
			_	_	on. An a					
			could	use the	vulnera	bility				
					se availa	-				
CV Scoring Scal	e O.	1.2	2.2	2.4	4.5	Г.С	C 7	7.0	0.0	0.40
(CVSS)	0-1 pe(s): CSRF- Cross	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Des	scription & CVE	ID	Pat	tch	NCIIP	PC ID
			advisory public e	ce. At the time publication reploitation of vulnerability	no this				
			CVE ID :	CVE-2019-6	568				
sinamics_s21	0_firmware								
Improper Input Validation	17-04-2019	5	identified versions versions (All versions (All versions (All versions OPC UA SIMATIO Controll (All versions Comfort 15" (All versions KTP Mol KTP700 und KTP SIMATIO (All versions (All	rability has beed in CP1604 (as), CP1616 (Al si), SIAMTIC RISIONS), SIMATIC CRISIONS, SIMATIC CRISIONS	All I I I I I I I I I I I I I I I I I I	N/A		O-SIE-S 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	С	escriptio	on & CVE	ID	Pa	tch	NCII	PC ID
			SIMAT	IC RF6	OR (All					
			versio	ns), SIM	IATIC S7	7-1500				
			CPU fa	mily (A	ll versio	ns),				
			SIMAT	TIC S7-1	500 Sof	tware				
			Contro	oller (Al	l versioi	1s),				
			SIMAT	'IC S7-3	00 CPU	family				
			(All ve	rsions	< V3.X.1	6),				
			SIMAT	TIC S7-4	00 PN (i	incl. F)				
			V6 and	d below	(All ver	sions),				
					00 PN/I	-				
			(incl. I	F) (All v	ersions)	,				
			SIMAT	CIC S7-P	LCSIM					
			Advan	ced (All	version	ıs).				
				IC Tele		<i>,</i>				
			Adapt	er IE Ad	vanced	(All				
			•	ns), SIM						
				-	dapter II	E Basic				
					SIMAT					
			_	_	dapter II					
					version					
				•	AC RTX	-				
					SIMAT					
			`	-	ne Adva					
					SIMOC					
			-	-	version					
			_	-	o V PN (-				
				•	AMICS (•				
				All vers		3150				
			`		30 V4.7	(A11				
					AMICS (•				
				-	versions					
				•		· .				
					30 V4.8	•				
					8 HF6),					
					30 V5.1	•				
					AMICS (
			V5.1 SP1 (All versions < V5.1 SP1 HF4), SINAMICS G150							
						J15U				
			`	All versi IICS G1	ons), 50 V4.7	(All				
CV Scoring Scale	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross									

Vulnerability Type(s)	Publish Date	cvss	De	scription & CVE	ID	Pat	tch	NCIII	PC ID	
			versions	s), SINAMICS	G150					
			V4.7 SP:	1 (All version	s),					
			SINAMI	CS G150 V4.8	(All					
			versions	s < V4.8 HF6)						
			SINAMI	CS G150 V5.1	(All					
			versions	s), SINAMICS	G150					
			V5.1 SP	1 (All version	s < V5.1					
			SP1 HF4), SINAMICS	S120					
			V4.6 (Al	l versions),						
			SINAMI	CS S120 V4.7	(All					
			versions	s), SINAMICS	S120					
			V4.7 SP:	1 (All version	s),					
				CS S120 V4.8	-					
				s < V4.8 HF6)	-					
				CS S120 V5.1						
				s), SINAMICS	-					
				1 (All version						
), SINAMICS						
				l versions),						
			`	CS S150 V4.7	(All					
				s), SINAMICS	•					
				1 (All version						
				CS S150 V4.8	-					
				s < V4.8 HF6)	-					
				CS S150 V5.1						
				s), SINAMICS	-					
				1 (All version						
				l (All Version l), SINAMICS						
				l versions),	3210					
			`	CS S210 V5.1	CD1					
					SF 1					
			-	sions), SITOP r (All version	a)					
					8),					
				SU8600 (All	1600					
				s), SITOP UPS						
			`	sions), TIM 15	31 IKC					
			`	sions). The						
	webserver of the affected									
				contains a	1 1					
			vulnera	bility that ma	y lead					
CV Scoring Sca	le 0-1	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10	
(CVSS) Vulnerability Ty										

Improper Input 17-04- Validation	vare
Improper Input 17-04-	vare
Input 17-04-	
vanuation	-2019 5
CV Scoring Scale (CVSS)	

Vulnerability Type(s)	Publish Date	cvss	Description & CVI	E ID Pa	atch	NCIIF	PC ID
			(All versions), SIMAT	IC HMI			
			Comfort Outdoor Par	iels 7" &			
			15" (All versions), SI	MATIC			
			HMI Comfort Panels	4" - 22"			
			(All versions), SIMAT	'IC HMI			
			KTP Mobile Panels K	ГР400F,			
			KTP700, KTP700F, K	TP900			
			und KTP900F (All ve	rsions),			
			SIMATIC IPC DiagMo	nitor			
			(All versions), SIMAT	'IC			
			RF181-EIP (All version	ons),			
			SIMATIC RF182C (Al	l			
			versions), SIMATIC R	F186C			
			(All versions), SIMAT	'IC			
			RF188C (All versions),			
			SIMATIC RF600R (Al	ĺ			
			versions), SIMATIC S	7-1500			
			CPU family (All versi	ons),			
			SIMATIC S7-1500 So	ftware			
			Controller (All version	ns),			
			SIMATIC S7-300 CPU	-			
			(All versions < V3.X.1	.6),			
			SIMATIC S7-400 PN	incl. F)			
			V6 and below (All ve				
			SIMATIC S7-400 PN/				
			(incl. F) (All versions				
			SIMATIC S7-PLCSIM	,,			
			Advanced (All versio	ns).			
			SIMATIC Teleservice	-5,			
			Adapter IE Advanced	(All			
			versions), SIMATIC				
			Teleservice Adapter	E Basic			
			(All versions), SIMAT				
			Teleservice Adapter				
			Standard (All version				
			SIMATIC WinAC RTX				
			(All versions), SIMAT				
WinCC Runtime Advanced							
			(All versions), SIMO				
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-1
(CVSS) Vulnerability Ty					, ,		

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE	ID	Pa	tch	NCIII	PC ID
			pro V EIP (Al	l version:	s),				
			SIMOCODE p	ro V PN (All				
			versions), SII	NAMICS (130				
			V4.6 (All vers	sions),					
			SINAMICS G1	30 V4.7 (All				
			versions), SII						
			V4.7 SP1 (All	versions),				
			SINAMICS G1	30 V4.8 (
			versions < V	l.8 HF6),					
			SINAMICS G1	30 V5.1 (All				
			versions), SII	NAMICS (130				
			V5.1 SP1 (All	versions	< V5.1				
			SP1 HF4), SII	NAMICS C	150				
			V4.6 (All vers	sions),					
			SINAMICS G1	50 V4.7 (All				
			versions), SII	NAMICS C	150				
			V4.7 SP1 (All	versions),				
		SINAMICS G150 V4.8 (All							
			versions < V4.8 HF6),						
			SINAMICS G1						
			versions), SII	NAMICS (
			V5.1 SP1 (All	versions	< V5.1				
			SP1 HF4), SII						
			V4.6 (All vers						
			SINAMICS S1		All				
			versions), SII	`					
			V4.7 SP1 (All						
			SINAMICS S1		,				
			versions < V	`					
			SINAMICS S1		All				
			versions), SII	`					
			V5.1 SP1 (All						
			SP1 HF4), SII						
			V4.6 (All vers						
			SINAMICS S1						
			versions), SII	`					
			V4.7 SP1 (All						
			SINAMICS S1						
	version				<i>1</i> 111				
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-1
(CVSS)	V 1		5 4		5 5	0,	, 0		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SINAMICS S150 V5.1 (All		
			versions), SINAMICS S150		
			V5.1 SP1 (All versions < V5.1		
			SP1 HF4), SINAMICS S210		
			V5.1 (All versions),		
			SINAMICS S210 V5.1 SP1		
			(All versions), SITOP		
			Manager (All versions),		
			SITOP PSU8600 (All		
			versions), SITOP UPS1600		
			(All versions), TIM 1531 IRC		
			(All versions). The		
			webserver of the affected		
			devices contains a		
			vulnerability that may lead		
			to a denial-of-service		
			condition. An attacker may		
			cause a denial-of-service		
			situation which leads to a		
			restart of the webserver of		
			the affected device. The		
			security vulnerability could		
			be exploited by an attacker		
			with network access to the		
			affected systems. Successful		
			exploitation requires no		
			system privileges and no		
			user interaction. An attacker		
			could use the vulnerability		
			to compromise availability of		
			the device. At the time of		
			advisory publication no		
			public exploitation of this		
			security vulnerability was		
			known.		
			CVE ID: CVE-2019-6568		
sitop_ups160	0_firmware				

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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2 (All versions), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions), SIMATIC HMI Comfort Panels 4" - 22" (All versions), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 und KTP900F (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF186C (All versions), SIMATIC RF186C (All versions), SIMATIC RF186C (All versions), SIMATIC RF186C (All versions), SIMATIC S7-1500 CPU family (All versions), SIMATIC S7-1500 CPU family (All versions), SIMATIC S7-300 CPU family (All versions), SIMATIC S7-400 PN (incl. F)	N/A	O-SIE-SITO- 010519/433
CV Scoring Sca	ole 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss	Description &	CVE ID	Pat	ch	NCIII	PC ID	
			V6 and below (All	versions),					
			SIMATIC S7-400 F	N/DP V7					
			(incl. F) (All version	ons),					
			SIMATIC S7-PLCS	M					
			Advanced (All ver	sions),					
			SIMATIC Teleserv	ice					
			Adapter IE Advan	ced (All					
			versions), SIMATI	C					
			Teleservice Adapt	Teleservice Adapter IE Basic					
			(All versions), SIM	ATIC					
			Teleservice Adapt	er IE					
			Standard (All vers	ions),					
			SIMATIC WinAC R						
			(All versions), SIM						
			WinCC Runtime A						
			(All versions), SIM						
			pro V EIP (All vers						
			SIMOCODE pro V	-					
			versions), SINAMI						
			V4.6 (All versions)						
			SINAMICS G130 V						
			versions), SINAMI						
			V4.7 SP1 (All vers						
			SINAMICS G130 V	-					
			versions < V4.8 Hl						
				,					
			SINAMICS G130 V	•					
			versions), SINAMI						
			V5.1 SP1 (All vers						
			SP1 HF4), SINAMI						
			V4.6 (All versions)						
			SINAMICS G150 V						
			versions), SINAMI						
			V4.7 SP1 (All vers	-					
			SINAMICS G150 V	•					
			versions < V4.8 HI	•					
			SINAMICS G150 V	-					
			versions), SINAMI						
			V5.1 SP1 (All vers						
			SP1 HF4), SINAMI	CS S120					
CV Scoring Sca	e 0-1	1-2	2-3 3-4 4-	5 5-6	6-7	7-8	8-9	9-10	
(CVSS)	0-1	1-2	3-4 4-	3-0	0-7	7-0	0-3	9-10	

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pate	ch	NCIII	PC ID	
			V4.6 (All versions),					
			SINAMICS S120 V4.7 (All					
			versions), SINAMICS S120					
			V4.7 SP1 (All versions),					
			SINAMICS S120 V4.8 (All					
			versions < V4.8 HF6),					
			SINAMICS S120 V5.1 (All					
			versions), SINAMICS S120					
			V5.1 SP1 (All versions < V	5.1				
			SP1 HF4), SINAMICS S150					
			V4.6 (All versions),					
			SINAMICS S150 V4.7 (All					
			versions), SINAMICS S150					
			V4.7 SP1 (All versions),					
			SINAMICS S150 V4.8 (All					
			versions < V4.8 HF6),					
			SINAMICS S150 V5.1 (All					
			versions), SINAMICS \$150					
			V5.1 SP1 (All versions < V	5.1				
			SP1 HF4), SINAMICS S210					
			V5.1 (All versions),					
			SINAMICS S210 V5.1 SP1					
			(All versions), SITOP					
			Manager (All versions),					
			SITOP PSU8600 (All					
			versions), SITOP UPS1600					
			(All versions), TIM 1531 I					
			(All versions). The					
			webserver of the affected					
			devices contains a					
			vulnerability that may lead	d				
			to a denial-of-service					
			condition. An attacker may	.,				
			cause a denial-of-service					
			situation which leads to a					
			restart of the webserver o	f				
			the affected device. The	•				
			security vulnerability coul	d				
			be exploited by an attacke					
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-	6 6-7	7-8	8-9	9-10	
(CVSS)	pe(s): CSRF- Cross		3 13 3					

Vulnerability Type(s)	Publish Date	cvss	ı	Descriptio	on & CVE	ID	Pa	tch	NCII	PC ID
			affectors explored system user is could to continue de advisor public security know	ed syste tation renteraction renteraction use the exploit exploit ty vulner.	access to ms. Success to ms. Success and con. An access and con. An access are available time time access to of cerability 2019-6	cessful no no ttacker bility bility of e of no this was				
simatic_hmi_k	ktp_mobile_pa	anels_k				300				
Improper Input Validation	ut 17-04-2019 5				y has be EP1604 (EP1	All I F185C IC IC III P443-1 IC III P443-1 IC III PPPC IC HMI IC	N/A		O-SIE- 01051	SIMA- 9/434
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descr	iption & CVE	ID	Pa	tch	NCIII	PC ID
			SIMATIC I	PC DiagMor	itor				
			(All versio	ns), SIMAT	C				
			RF181-EIF	(All versio	ns),				
			SIMATIC R	F182C (All	-				
			versions),	SIMATIC RI	F186C				
			(All versio	ns), SIMAT	C				
			RF188C (A	ll versions)	,				
			SIMATIC R	F600R (All					
			versions),	SIMATIC S7	'-1500				
			CPU family	(All versio	ns),				
			SIMATIC S	7-1500 Sof	tware				
			Controller	(All version	ıs),				
			SIMATIC S	7-300 CPU	family				
			(All versio	ns < V3.X.1	6),				
			`	7-400 PN (i	-				
			V6 and bel	ow (All ver	sions),				
				7-400 PN/I					
		(incl. F) (All versions),							
			SIMATIC S	_					
			Advanced	(All version	ıs),				
			SIMATIC Teleservice						
			Adapter IE						
			versions),						
			-	e Adapter II	E Basic				
				ns), SIMATI					
			`	e Adapter II					
				All versions					
			`	VinAC RTX	-				
				ns), SIMAT					
			-	ntime Adva					
				ns), SIMOC					
			`	All version					
			-	E pro V PN (-				
				SINAMICS (
			Versions), V4.6 (All v						
			`	G130 V4.7					
				SINAMICS (
				All versions					
		SINAMICS							
CV Scoring Sca	le 0-1	1-2	2-3 3-4	1 4-5	5-6	6-7	7-8	8-9	9-1
(CVSS)	<u> </u>				3 0	J ,	, ,	5 5	1

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE I	D	Pa	tch	NCIII	PC ID
			versions < V	1.8 HF6),					
			SINAMICS G1	30 V5.1 (All				
			versions), SII	NAMICS G	130				
			V5.1 SP1 (All	versions	< V5.1				
			SP1 HF4), SII	NAMICS G	150				
			V4.6 (All ver	sions),					
			SINAMICS G1	50 V4.7 (All				
			versions), SII	NAMICS G	150				
			V4.7 SP1 (All	versions),				
			SINAMICS G1	50 V4.8 (All				
			versions < V	4.8 HF6),					
			SINAMICS G1	50 V5.1 (All				
			versions), SII	NAMICS G	150				
			V5.1 SP1 (All						
			SP1 HF4), SII						
			V4.6 (All ver						
			SINAMICS S1	-	All				
			versions), SII	•					
			V4.7 SP1 (All						
			SINAMICS S1	-					
			versions < V	•					
			SINAMICS S1		All				
			versions), SII	•					
			V5.1 SP1 (All						
			SP1 HF4), SII						
			V4.6 (All vers		100				
			SINAMICS S1	J .	All				
			versions), SII	•					
			V4.7 SP1 (All						
			SINAMICS S1	-					
			versions < V	•	AII				
					۸11				
			SINAMICS S1	•					
			versions), SII						
			V5.1 SP1 (All						
			SP1 HF4), SINAMICS S210						
			V5.1 (All versions), SINAMICS S210 V5.1 SP1						
					71				
			(All versions Manager (All).				
CV Scoring Scal			Tranager (TIII	, 0.1.0110113	,, 				
(CVSS)	0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

SITOP PSU8600 (All versions), SITOP UPS1600 (All versions), SITOP UPS1600 (All versions), SITOP UPS1600 (All versions), SITOP UPS1600 (All versions), TIM 1531 IRC (All versions), The webserver of the affected devices contains a vulnerability that may lead to a denial-of-service condition. An attacker may cause a denial-of-service situation which leads to a restart of the webserver of the affected device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID : CVE-2019-6568 Simatic_hmi_ktp_mobile_panels_ktp900_firmware A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIMATIC (CP443-1 Advanced (All versions), SIMATIC (CP443-1 Advanced (All versions), SIMATIC (CP443-	Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
Improper Input Validation 17-04-2019 5 A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 Advanced (All versions), SIMATIC CP443-1 Advance				version (All von (All von (All von (All von (All von vulne)) to a discondification of the affect of the design of	ersions) ersions) ersions) erver of es conta rability enial-of- tion. An a denial ion whice fected d ity vulne oloited b network ed syste itation r n privile use the npromis evice. At ory publ c exploit ity vulne ity	OP UPS1 TIM 15 The the affectins a that may service attacker electrical representation of the time attaction of the attaction	31 IRC cted v lead v lead v may ice to a ver of ne could acker o the cessful no no ttacker bility bility of e of no this was				
identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC (CP343-1 Advanced (All versions), SIMATIC (All versions), SIMATIC (CP443-1 (All versions), SIMATIC (CP443-1 Advanced (All versions), SIMATIC	simatic_hmi_k	ctp_mobile_pa	nels_k	tp900	_firmwa	re					
- I I I I I I I I I I I I I I I I I I I	Input	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC				N/A			
	_	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description	n & CVE ID	Pa	tch	NCIII	PC ID
			versions), SIMA	ATIC CP443-1				
			OPC UA (All ve	rsions),				
			SIMATIC ET 20	00 SP Open				
			Controller CPU	1515SP PC				
			(All versions <	V2.1.6),				
			SIMATIC ET 20	00 SP Open				
			Controller CPU	1515SP PC2				
			(All versions),	SIMATIC HMI				
			Comfort Outdo	or Panels 7" 8	ž.			
			15" (All version	ns), SIMATIC				
			HMI Comfort P	-				
			(All versions),	SIMATIC HMI				
			KTP Mobile Pa					
			KTP700, KTP7		ĺ			
			und KTP900F (
			SIMATIC IPC D	,				
			(All versions),	· ·				
			RF181-EIP (All					
			SIMATIC RF18	-				
			versions), SIMA					
			(All versions),					
			RF188C (All ve					
			SIMATIC RF60	-				
			versions), SIMA	-				
			CPU family (All					
			SIMATIC S7-15					
			Controller (All	-				
			SIMATIC S7-30	,				
			(All versions <	-				
			SIMATIC S7-40	,				
			V6 and below (
			SIMATIC S7-40	•				
			(incl. F) (All ve	3 .				
			SIMATIC S7-PLCSIM					
			Advanced (All					
			SIMATIC Teles					
			Adapter IE Adv					
			versions), SIMATIC					
			Teleservice Ad	apter IE Basic				
CV Scoring Sca	e 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)	0-1	1-2	2-3 3-4	4-5	0-7	7-0	0-3	3-10

Vulnerability Type(s)	Publish Date	cvss	Description & C	/E ID Pa	itch	NCIII	PC ID
			(All versions), SIMA	TIC			
			Teleservice Adapter	IE			
			Standard (All version	ns),			
			SIMATIC WinAC RT	X 2010			
			(All versions), SIMA	TIC			
			WinCC Runtime Adv	vanced			
			(All versions), SIMO	CODE			
			pro V EIP (All version	ons),			
			SIMOCODE pro V Pi	l (All			
			versions), SINAMIC	S G130			
			V4.6 (All versions),				
			SINAMICS G130 V4.	7 (All			
			versions), SINAMIC	S G130			
			V4.7 SP1 (All versio				
			SINAMICS G130 V4.	,			
			versions < V4.8 HF6	•			
			SINAMICS G130 V5.	*			
			versions), SINAMIC	`			
			V5.1 SP1 (All versio				
			SP1 HF4), SINAMIC				
			V4.6 (All versions),				
			SINAMICS G150 V4.	7 (All			
			versions), SINAMIC	•			
			V4.7 SP1 (All version				
			SINAMICS G150 V4.	,			
			versions < V4.8 HF6				
			SINAMICS G150 V5.	· .			
			versions), SINAMIC	•			
			V5.1 SP1 (All version				
			•				
			SP1 HF4), SINAMIC	5 5120			
			V4.6 (All versions),	7 (4 1)			
			SINAMICS S120 V4.	•			
			versions), SINAMIC				
			V4.7 SP1 (All versio	•			
			SINAMICS S120 V4.	•			
			versions < V4.8 HF6	•			
			SINAMICS S120 V5.	•			
			versions), SINAMIC V5.1 SP1 (All versio				
CV Scoring Scal	<u> </u>		vo.1 or 1 (All versio	113 > V J.1			
(CVSS)	0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	С	escriptio	on & CVE	ID	Pa	tch	NCIII	PC ID
			SP1 H	F4), SIN	AMICS S	5150				
			V4.6 (All vers	ions),					
			SINAM	IICS S15	50 V4.7	(All				
			versio	ns), SIN	AMICS S	S150				
			V4.7 S	P1 (All	versions	s),				
			SINAM	IICS S15	50 V4.8	(All				
			versio	ns < V4	.8 HF6),					
			SINAM							
			versio	ns), SIN						
			V5.1 S	P1 (All	versions	s < V5.1				
			SP1 H	F4), SIN	AMICS S	5210				
			V5.1 (All vers	ions),					
			SINAM	IICS S21	L0 V5.1	SP1				
			(All ve	rsions)	SITOP					
			`	-	versions	;),				
			_	PSU860		,				
					OP UPS:	1600				
				-	TIM 15					
			`	rsions)						
			`	_	the affe	cted				
			device	s conta	ins a					
			vulner	ability	that may	lead				
				_	service					
			condit	ion. An	attackei	may				
					-of-serv	-				
			situati	on whic	ch leads	to a				
			restar	t of the	webserv	er of				
			the aff	ected d	evice. Tł	ne				
					erability					
				•	y an att					
			•		access t					
					ms. Succ					
				-	equires					
			_		_					
			system privileges and no user interaction. An attacker							
			could use the vulnerability							
						bility of				
				-	the time	-				
					ication i	-				
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross									

Vulnerability Type(s)	Publish Date	cvss	ı	Descriptio	on & CVE	ID	Pa	itch	NCII	PC ID
			_	exploit ty vulne n.						
				D : CVE-		568				
simatic_hmi_k	ktp_mobile_pa	nels_k	_							
Improper Input Validation	17-04-2019	5	identi versio (All ve CP343 versio (All ve CP443 versio OPC U SIMA' Contr (All ve SIMA' Contr (All ve KTP N KTP7 und K SIMA' (All ve RF183 SIMA' versio (All ve RF183 SIMA'	rerability fied in Cons), CP1 ons), SIA ersions), 3-1 Adva ons), SIM ersions), 3-1 Adva ons), SIM ersions, GIC ET 2 coller CP ersions < Comfort ersions), ort Outd All versio Comfort ersions), ort Outd Comfort ersions), ort Outd Comfort ersions), ort Outd All versio Ersions), ort Outd Comfort ersions), ort Outd Comfor	P1604 (A) 616 (A) MTIC R) SIMAT Inced (A) IATIC CI PRISON OF O U 1515S V2.1.6 OO SP O U 1515S V2.1.6 OOF, KI Panels KI OOF, KI (All versions) SIMAT IN (All versions) SIMAT CALL CALL CALL CALL CALL CALL CALL CA	(All all all all all all all all all all	N/A			SIMA- 9/436
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 Typ	pe(s): CSRF- Cross Denial of Service	_	_			_				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Des	cription & CVE	ID	Pa	tch	NCIII	PC ID
			CPU fam	ily (All versio	ns),				
			SIMATIO	S7-1500 Soft	ware				
			Controll	er (All version	ıs),				
				S7-300 CPU	-				
			(All vers	ions < V3.X.16	5),				
			`	S7-400 PN (i					
				elow (All ver	_				
				S7-400 PN/I	-				
				(All versions)					
			,	S7-PLCSIM	,				
				d (All version	s).				
				Teleservice	,				
				IE Advanced	(A))				
			_), SIMATIC	(1111				
				rice Adapter II	Rasic				
				ions), SIMATI					
			`	rice Adapter II					
				d (All versions					
				C WinAC RTX					
				ions), SIMATI					
			`	tuntime Adva					
				ions), SIMOC(
				P (All version					
				DE pro V PN (
), SINAMICS (ı130				
			`	l versions),	C A 11				
				CS G130 V4.7	`				
), SINAMICS (
				(All versions					
				CS G130 V4.8	(All				
				< V4.8 HF6),					
				CS G130 V5.1	`				
			versions), SINAMICS (G130				
			V5.1 SP1	(All versions	< V5.1				
			SP1 HF4), SINAMICS (G150				
			V4.6 (Al	l versions),					
			SINAMI	CS G150 V4.7	(All				
			versions), SINAMICS (G150				
			V4.7 SP1	(All versions),				
CV Scoring Sca	le 0.1	1.3	2.3	2.4	F. C	6.7	7.0	0.0	ا م
(CVSS)	0-1	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-1

Vulnerability Type(s)	Publish Date	cvss	Des	cription & CVE	ID	Pa	tch	NCIII	PC ID
			SINAMIC	S G150 V4.8	(All				
			versions	< V4.8 HF6),					
			SINAMIC	S G150 V5.1	(All				
			versions), SINAMICS (G150				
			V5.1 SP1	(All versions	< V5.1				
			SP1 HF4), SINAMICS S	120				
			V4.6 (All	versions),					
			SINAMIC	S S120 V4.7 (All				
			versions), SINAMICS S	120				
			<u> </u>	(All versions					
				S S120 V4.8 (-				
				< V4.8 HF6),					
				S S120 V5.1 (All				
), SINAMICS S	•				
			<u> </u>	(All versions					
), SINAMICS S					
			<u> </u>	versions),					
			_	S S150 V4.7 (
), SINAMICS S					
			<u> </u>	(All versions					
				S S150 V4.8 (-				
				< V4.8 HF6),					
				S S150 V5.1 (All				
), SINAMICS S	•				
			1	(All versions					
), SINAMICS S					
				versions),	1210				
			`	S S210 V5.1 S	SD1				
					or 1				
			-	ions), SITOP	,				
				(All versions	ا,				
				SU8600 (All	600				
			<u> </u>), SITOP UPS1					
			`	ions), TIM 15	31 IKC				
			`	ions). The					
				er of the affec	ted				
				ontains a	, .				
				ility that may	lead				
				al-of-service					
			conditio	n. An attacker	may				
CV Scoring Sca	le 0-1	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-1
(CVSS)	0 1		2 3	1 13	3.0	0 /	, 0		

					on & CVE		itch		PC ID	
	ntic_rf181-eip_firmware		situation restarthe affice exploising system user in could to continue deadvise public	evice. At ory publ e exploit ty vulne	ch leads webservevice. The rability of an atternation of atternation attends	to a ver of ne could acker to the cessful no no ttacker bility bility of e of no this				
simatic rf181.	oin firmwar	Δ	CVE II	D : CVE-	2019-6	568				
Simatic_rf181-eip_firmware A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 Advanced (All N/A)										SIMA- 9/437
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)	Publish Date	cvss	Descrip	tion & CVE	ID	Pa	tch	NCIII	PC ID
			15" (All ver	sions), SIN	1ATIC				
			HMI Comfor	t Panels 4	-" - 22"				
			(All version	s), SIMAT	IC HMI				
			KTP Mobile	Panels K1	'P400F,				
			KTP700, KT	P700F, K	ГР900				
			und KTP900	F (All ver	sions),				
			SIMATIC IPO	C DiagMor	nitor				
			(All version	s), SIMAT	IC				
			RF181-EIP (All versio	ns),				
			SIMATIC RF	182C (All					
			versions), S	MATIC R	F186C				
			(All version	s), SIMAT	IC				
			RF188C (All	versions),				
			SIMATIC RF	600R (All					
			versions), S	-					
			CPU family	All version					
			SIMATIC S7	-1500 Sof					
			Controller (All version					
			SIMATIC S7	-300 CPU					
			(All version	s < V3.X.1					
			SIMATIC S7	-400 PN (incl. F)				
			V6 and belo	w (All ver	sions),				
			SIMATIC S7	•	-				
			(incl. F) (All	•					
			SIMATIC S7	-PLCSIM					
			Advanced (A	All versior	ıs),				
			SIMATIC Te		,				
			Adapter IE A	Advanced	(All				
			versions), S						
			Teleservice		E Basic				
			(All version	-					
			Teleservice	J.					
			Standard (A	•					
			SIMATIC Wi		•				
			(All version						
			WinCC Runt	-					
			(All version						
			pro V EIP (A						
			SIMOCODE		-				
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-1
(CVSS) Vulnerability Ty									

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PCID
			versic	ns), SIN	AMICS (G130				
				All vers						
			`		30 V4.7	(All				
					AMICS (`				
				-	versions					
				•	30 V4.8	-				
				ns < V4						
			SINAN	MICS G1	30 V5.1	(All				
					AMICS (`				
				-	versions					
				•	AMICS (
				All vers						
					50 V4.7	(All				
					AMICS (-				
				-	versions					
				•	50 V4.8	-				
				ns < V4						
					50 V5.1					
			versio	ns), SIN	AMICS (
			V5.1 S	SP1 (All	versions	< V5.1				
			SP1 H	F4), SIN	AMICS S	5120				
			V4.6 (All vers	ions),					
					20 V4.7 (All				
					AMICS S	•				
				-	versions					
			SINAN	AICS S12	20 V4.8 (All				
				ns < V4		•				
					20 V5.1 (All				
					AMICS S	•				
					versions					
				-	AMICS S					
				All vers						
			`		50 V4.7 (All				
					AMICS S	•				
					versions					
				•	50 V4.8 (-				
					.8 HF6),	-				
					50 V5.1 (
			versions), SINAMICS S150							
CV Scoring Sca	le le			-		-	1			
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			SP1 H V5.1 (SINAM (All ve Manag SITOF version (All ve (All ve webse device vulne to a de condir cause situat restar the aff securi be exp with r affecte exploit syster user in could to con the de advise public	evice. At ory publ e exploit ity vulne	AMICS Sions), 10 V5.1; 10 V5.1; 10 V5.1; 10 V5.1; 10 V5.1; 10 V6.1 10	SP1				
simatic_rf182	c firmware		CVEI	D : CVE-	2019-6	508				
	-		A vulr	nerabilit	y has be	en			O CIE	CIMA
Improper Input	17-04-2019	5	identified in CP1604 (All versions), CP1616 (All				N/A			-SIMA- 19/438
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_	_			_			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descrip	ion & CVE	ID	Pat	tch	NCIII	PC ID
Validation			versions), SI	AMTIC RI	7185C				
			(All versions	s), SIMATI	C				
			CP343-1 Ad	vanced (A	ll				
			versions), SI	MATIC CF	443-1				
			(All versions	s), SIMATI	C				
			CP443-1 Ad	vanced (A	ll				
			versions), SI	MATIC CF	443-1				
			OPC UA (All	versions)	1				
			SIMATIC ET	200 SP O	pen				
			Controller C	PU 1515S	P PC				
			(All versions	s < V2.1.6)	,				
			SIMATIC ET	200 SP O	pen				
			Controller C	PU 1515S	P PC2				
			(All versions	s), SIMATI	C HMI				
			Comfort Out	door Pane	els 7" &				
			15" (All vers	ions), SIM	IATIC				
			HMI Comfor	t Panels 4	" - 22"				
			(All versions	s), SIMATI	C HMI				
			KTP Mobile	Panels KT	P400F,				
			KTP700, KT	P700F, KT	'P900				
			und KTP900	F (All ver	sions),				
			SIMATIC IPO	DiagMon	itor				
			(All versions	s), SIMATI	С				
			RF181-EIP (All versio	ns),				
			SIMATIC RF	182C (All					
			versions), SI	MATIC RI	7186C				
			(All versions	s), SIMATI	C				
			RF188C (All	versions)	,				
			SIMATIC RF	600R (All					
			versions), SI	MATIC S7	-1500				
			CPU family (All versio	ns),				
			SIMATIC S7-	1500 Soft	ware				
			Controller (A	All version	ıs),				
			SIMATIC S7-	300 CPU	family				
			(All versions	s < V3.X.16	5),				
			SIMATIC S7-	400 PN (i	ncl. F)				
			V6 and belo	w (All ver	sions),				
			SIMATIC S7-	400 PN/I					
			(incl. F) (All	versions)	<u>, </u>				
CV Scoring Scal	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross								

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC S7-PLCSIM		
			Advanced (All versions),		
			SIMATIC Teleservice		
			Adapter IE Advanced (All		
			versions), SIMATIC		
			Teleservice Adapter IE Basic	c	
			(All versions), SIMATIC		
			Teleservice Adapter IE		
			Standard (All versions),		
			SIMATIC WinAC RTX 2010		
			(All versions), SIMATIC		
			WinCC Runtime Advanced		
			(All versions), SIMOCODE		
			pro V EIP (All versions),		
			SIMOCODE pro V PN (All		
			versions), SINAMICS G130		
			V4.6 (All versions),		
			SINAMICS G130 V4.7 (All		
			versions), SINAMICS G130		
			V4.7 SP1 (All versions),		
			SINAMICS G130 V4.8 (All		
			versions < V4.8 HF6),		
			SINAMICS G130 V5.1 (All		
			versions), SINAMICS G130		
			V5.1 SP1 (All versions < V5.)	1	
			`	1	
			SP1 HF4), SINAMICS G150		
			V4.6 (All versions),		
			SINAMICS G150 V4.7 (All		
			versions), SINAMICS G150		
			V4.7 SP1 (All versions),		
			SINAMICS G150 V4.8 (All		
			versions < V4.8 HF6),		
			SINAMICS G150 V5.1 (All		
			versions), SINAMICS G150		
			V5.1 SP1 (All versions < V5.	1	
			SP1 HF4), SINAMICS S120		
			V4.6 (All versions),		
			SINAMICS S120 V4.7 (All		
			versions), SINAMICS S120		
CV Scoring Sca	e 0.4	1.2	22 24 45 56	6.7	80 01
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss	Descri	ption & CVE	ID	Pa	tch	NCIII	PC ID
			V4.7 SP1 (A	All versions	;),				
			SINAMICS	S120 V4.8	(All				
			versions <	V4.8 HF6),					
			SINAMICS	S120 V5.1	(All				
			versions), S	SINAMICS S	5120				
			V5.1 SP1 (A	All versions	s < V5.1				
			SP1 HF4), S	SINAMICS S	5150				
			V4.6 (All ve	ersions),					
			SINAMICS	S150 V4.7	(All				
			versions), S	SINAMICS S	S150				
			V4.7 SP1 (A	All versions	s),				
			SINAMICS		-				
			versions <		•				
			SINAMICS	-					
			versions), S		-				
			V5.1 SP1 (A						
			SP1 HF4), S						
			V5.1 (All ve						
			SINAMICS	-					
			(All version		J1 1				
			Manager (A	-	:)				
			SITOP PSU		יני				
			versions), S	•	1600				
			(All version						
			(All version	-	JIIII				
			webserver	-	rtad				
			devices cor		leu				
			vulnerabili		, load				
			to a denial-		/ leau				
			condition.		•				
			cause a der						
			situation w						
			restart of t						
			the affected						
			security vu	-					
			be exploite	-					
			with netwo						
			affected sy						
			exploitatio	n requires	no				
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCII	PC ID
			user i could to cor the de advise public secur know	m privile nteractic use the mpromis evice. At ory publ c exploit ity vulne n. D: CVE-	on. An at vulneral e availal the time ication r ation of erability	ttacker bility bility of e of no this was				
simatic_rf185	c_firmware									
Improper Input Validation	17-04-2019	5	identi versic (All versic (All versic (All versic (All versic OPC U SIMA' Contr (All versic Contr (All versic (All	nerabilitation (Cons), CP1 ons), SIA ersions), 3-1 Adva ons), SIM ersions), 3-1 Adva ons), SIM JA (All versions), ort CET 2 coller CP ersions (Comfort ersions) Mobile Pa TIC IPC I ersions) 1-EIP (A	P1604 (All MTIC RIMTIC RIMTIC RIMTIC RIMTIC RIMTIC CITES (ALL TERMINE) ([All I F185C IC IC IC IC IC IC IC	N/A		0-SIE- 01051	SIMA- 9/439
CV Scoring Scal (CVSS)	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1						6-7	7-8	8-9	9-10
	pe(s): CSRF- Cross Denial of Service	_							nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE	ID	Pa	tch	NCIII	PC ID
			SIMATIC RF	182C (All					
			versions), SI	MATIC RI	F186C				
			(All versions), SIMATI	C				
			RF188C (All	versions)	,				
			SIMATIC RF	600R (All					
			versions), SI	MATIC S7	'-1500				
			CPU family (All versio	ns),				
			SIMATIC S7-	1500 Sof	tware				
			Controller (A	All version	ıs),				
			SIMATIC S7-		-				
			(All versions		-				
			SIMATIC S7-		· .				
			V6 and below	•	_				
			SIMATIC S7-	•	,				
			(incl. F) (All	•					
			SIMATIC S7-	,	,				
			Advanced (A		s).				
			SIMATIC Tel		,				
			Adapter IE A		(All				
			versions), SI		(1111				
			Teleservice		E Basic				
			(All versions	-					
			Teleservice						
			Standard (A)	_					
			SIMATIC Wi						
			(All versions						
			WinCC Runt	,					
			(All versions	,					
			pro V EIP (A		•				
			SIMOCODE I	•	•				
			versions), SI		ı130				
			V4.6 (All ver		C A 11				
			SINAMICS G		•				
			versions), SI						
			V4.7 SP1 (Al		-				
			SINAMICS G		(All				
			versions < V	-					
			SINAMICS G						
			versions), SI	NAMICS (G130				
CV Scoring Scale	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross								

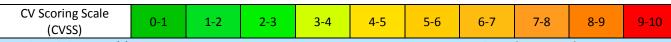
Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CVE	ID	Pa	tch	NCII	PC ID
			V5.1 SP1 (A	ll versions	s < V5.1				
			SP1 HF4), S	NAMICS (G150				
			V4.6 (All ve	rsions),					
			SINAMICS G	150 V4.7	(All				
			versions), S	NAMICS (G150				
			V4.7 SP1 (A	ll versions	s),				
			SINAMICS G	150 V4.8	(All				
			versions < V	4.8 HF6),					
			SINAMICS G	150 V5.1	(All				
			versions), S	NAMICS (G150				
			V5.1 SP1 (A	ll versions	s < V5.1				
			SP1 HF4), S	NAMICS S	5120				
			V4.6 (All ve	rsions),					
			SINAMICS S	120 V4.7	(All				
			versions), S	NAMICS S	5120				
			V4.7 SP1 (A	ll versions	s),				
			SINAMICS S	120 V4.8	(All				
			versions < V	4.8 HF6),					
			SINAMICS S	120 V5.1	(All				
			versions), S	NAMICS S	5120				
			V5.1 SP1 (A	ll versions	s < V5.1				
			SP1 HF4), S	NAMICS S	S150				
			V4.6 (All ve	rsions),					
			SINAMICS S	150 V4.7	(All				
			versions), S	NAMICS S	S150				
			V4.7 SP1 (A	ll versions	s),				
			SINAMICS S	150 V4.8	(All				
			versions < V	4.8 HF6),					
			SINAMICS S	150 V5.1	(All				
			versions), S	NAMICS S	S150				
			V5.1 SP1 (A	ll versions	s < V5.1				
			SP1 HF4), S						
			V5.1 (All ve						
			SINAMICS S	-	SP1				
			(All version	s), SITOP					
			Manager (A	s),					
			SITOP PSU8600 (All						
			versions), SITOP UPS1600						
			(All version						
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIII	PC ID
			(All versions). The webserver of the affected devices contains a vulnerability that may lead to a denial-of-service condition. An attacker may cause a denial-of-service situation which leads to a restart of the webserver of the affected device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6568				
simatic_rf186	c_firmware					-	
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 Advanced (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open	N/A		O-SIE- 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
	pe(s): CSRF- Cross	Site Rea	uest Forgery; Dir. Trav Directory Trav	ersal; +Inf	o- Gain Ir	nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE I	D	Pa	tch	NCII	PC ID
			Controller CI	U 1515SF	PC				
			(All versions	< V2.1.6),					
			SIMATIC ET	200 SP Op	en				
			Controller CI						
			(All versions), SIMATIO	CHMI				
			Comfort Out	door Pane	ls 7" &				
			15" (All versi	ons), SIM					
			HMI Comfort	Panels 4"					
			(All versions), SIMATIO					
			KTP Mobile I	anels KTI	P400F,				
			KTP700, KTF	700F, KT	P900				
			und KTP900	F (All vers	ions),				
			SIMATIC IPC	-					
			(All versions	•					
			RF181-EIP (A						
			SIMATIC RF1		- 57				
			versions), SII	•	186C				
			(All versions						
			RF188C (All						
			SIMATIC RF6	-					
			versions), SII	-	1500				
			CPU family (A						
			SIMATIC S7-		-				
			Controller (A						
			SIMATIC S7-		-				
			(All versions		•				
			SIMATIC S7-		· .				
			V6 and below	•	_				
			SIMATIC S7-	•					
			(incl. F) (All v	•	r v /				
				,					
			SIMATIC S7-						
			Advanced (A		iJ,				
			SIMATIC Tele		A 11				
			Adapter IE A	•	AII				
			versions), SII						
			Teleservice A						
			(All versions), SIMATIC						
			Teleservice A	•					
			Standard (All versions),						
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross								

Vulnerability Type(s)	Publish Date	cvss	Descripti	on & CVE	ID	Pat	tch	NCIII	PC ID
			SIMATIC Win	AC RTX 2	2010				
			(All versions)	, SIMATI	С				
			WinCC Runtii	ne Advai	nced				
			(All versions)	, SIMOCO	DDE				
			pro V EIP (All	version	s),				
			SIMOCODE pr	ro V PN (All				
			versions), SIN	IAMICS (
			V4.6 (All vers	ions),					
			SINAMICS G1	30 V4.7 (
			versions), SIN	IAMICS (G130				
			V4.7 SP1 (All	versions),				
			SINAMICS G1	30 V4.8 (All				
			versions < V4		•				
			SINAMICS G1	· ·	All				
			versions), SIN						
			V5.1 SP1 (All						
			SP1 HF4), SIN						
				ions),	.100				
			SINAMICS G1	-	(All				
			versions), SIN		•				
			V4.7 SP1 (All						
			SINAMICS G1		-				
			versions < V4		[7111				
			SINAMICS G1	-	Δ11				
					-				
			versions), SIN						
			V5.1 SP1 (All						
			SP1 HF4), SIN		120				
			V4.6 (All vers	-	· A 11				
			SINAMICS S1		•				
			versions), SIN						
			V4.7 SP1 (All		-				
			SINAMICS S1	`	All				
			versions < V4	,					
			SINAMICS S1		•				
			versions), SIN						
			V5.1 SP1 (All						
			SP1 HF4), SINAMICS S150 V4.6 (All versions),						
			SINAMICS S150 V4.7 (All						
CV Scoring Sca	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1		2 3 4	7 3	3 0	0 /	, 0	0 9	7 1

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			versions), SINAMICS S150		
			V4.7 SP1 (All versions),		
			SINAMICS S150 V4.8 (All		
			versions < V4.8 HF6),		
			SINAMICS S150 V5.1 (All		
			versions), SINAMICS S150		
			V5.1 SP1 (All versions < V5.1		
			SP1 HF4), SINAMICS S210		
			V5.1 (All versions),		
			SINAMICS S210 V5.1 SP1		
			(All versions), SITOP		
			Manager (All versions),		
			SITOP PSU8600 (All		
			versions), SITOP UPS1600		
			(All versions), TIM 1531 IRC		
			(All versions). The		
			webserver of the affected		
			devices contains a		
			vulnerability that may lead		
			to a denial-of-service		
			condition. An attacker may		
			cause a denial-of-service		
			situation which leads to a		
			restart of the webserver of		
			the affected device. The		
			security vulnerability could		
			be exploited by an attacker		
			with network access to the		
			affected systems. Successful		
			exploitation requires no		
			system privileges and no		
			user interaction. An attacker		
			could use the vulnerability		
			to compromise availability of		
			the device. At the time of		
			advisory publication no		
			public exploitation of this		
			security vulnerability was		



Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			know	n.						
			CVE I	D : CVE-	2019-6	568				
simatic_teles	ervice_adapte	r_ie_ad	lvance	d_firmw	are					
Improper Input Validation	17-04-2019	5	identi versic versic (All versic (All versic (All versic OPC U SIMA' Contr (All versic Comfe 15" (A HMI C (All versic	nerability fied in Cons), CP1 ons), SIA ersions), 3-1 Adva ons), SIM ersions), 3-1 Adva ons), SIM IA (All versions), ort Outd All versions), ort Outd Comfort ersions), ort Outd Comfor	P1604 (All MTIC RIAL SIMAT) anced (All ATIC CINTERS) oor Pan ons), SIMAT anels (All Verbiag More, SIMAT) anels (All Verbiag More, SIMAT) anels (All Verbiag More), SIMAT anels (All Verbiag Mo	[All I	N/A		O-SIE- 01051	SIMA- 9/441
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	() CCDT C	Cito Doo						· • •		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	tch	NCIII	PC ID
			Controller (All versions),				
			SIMATIC S7-300 CPU fam				
			(All versions < V3.X.16),				
			SIMATIC S7-400 PN (incl	l. F)			
			V6 and below (All version	ns),			
			SIMATIC S7-400 PN/DP V	-			
			(incl. F) (All versions),				
			SIMATIC S7-PLCSIM				
			Advanced (All versions),				
			SIMATIC Teleservice				
			Adapter IE Advanced (All	l l			
			versions), SIMATIC				
			Teleservice Adapter IE Ba	asic			
			(All versions), SIMATIC				
			Teleservice Adapter IE				
			Standard (All versions),				
			SIMATIC WinAC RTX 201	10			
			(All versions), SIMATIC				
			WinCC Runtime Advance	ed			
			(All versions), SIMOCODE				
			pro V EIP (All versions),				
			SIMOCODE pro V PN (All				
			versions), SINAMICS G13				
			V4.6 (All versions),				
			SINAMICS G130 V4.7 (All	ı			
			versions), SINAMICS G13				
			V4.7 SP1 (All versions),				
			SINAMICS G130 V4.8 (All	1			
			versions < V4.8 HF6),				
			SINAMICS G130 V5.1 (All	1			
			`				
			versions), SINAMICS G13				
			V5.1 SP1 (All versions < V				
			SP1 HF4), SINAMICS G15	00			
			V4.6 (All versions),	,			
			SINAMICS G150 V4.7 (All				
			versions), SINAMICS G15	00			
			V4.7 SP1 (All versions),	_			
			SINAMICS G150 V4.8 (All				
CV Scoring Scal			versions < V4.8 HF6),	 			
(CVSS)	0-1	1-2	2-3 3-4 4-5 5	5-6 6-7	7-8	8-9	9-1

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	tch	NCIII	PC ID	
			SINAMICS G150 V5.1 (All					
			versions), SINAMICS G15	0				
			V5.1 SP1 (All versions < V	75.1				
			SP1 HF4), SINAMICS S120)				
			V4.6 (All versions),					
			SINAMICS S120 V4.7 (All					
			versions), SINAMICS \$120)				
			V4.7 SP1 (All versions),					
			SINAMICS S120 V4.8 (All					
			versions < V4.8 HF6),					
			SINAMICS S120 V5.1 (All					
			versions), SINAMICS \$120)				
			V5.1 SP1 (All versions < V					
			SP1 HF4), SINAMICS S150					
			V4.6 (All versions),					
			SINAMICS S150 V4.7 (All					
			versions), SINAMICS S150)				
			V4.7 SP1 (All versions),					
			SINAMICS S150 V4.8 (All					
			versions < V4.8 HF6),					
			SINAMICS S150 V5.1 (All					
			versions), SINAMICS S150)				
			V5.1 SP1 (All versions < V					
			SP1 HF4), SINAMICS S210					
			V5.1 (All versions),					
			SINAMICS S210 V5.1 SP1					
			(All versions), SITOP					
			Manager (All versions),					
			SITOP PSU8600 (All					
			versions), SITOP UPS160	n				
			(All versions), TIM 1531					
			(All versions). The					
			webserver of the affected					
			devices contains a					
				.d				
			vulnerability that may lea	ıu				
			to a denial-of-service					
			condition. An attacker ma	ıy				
			cause a denial-of-service					
			situation which leads to a					
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5	-6 6-7	7-8	8-9	9-1	
(CVSS) Vulnerability Ty								

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			restart of the webserver of the affected device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.		
simatic_telese	ervice adante	r ie ha	CVE ID : CVE-2019-6568		
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2 (All versions), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions), SIMATIC HMI Comfort Panels 4" - 22"	N/A	O-SIE-SIMA- 010519/442
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	-8 8-9 9-10
		_	uest Forgery; Dir. Trav Directory Travo oss Site Scripting; Sql- SQL Injection; N 357		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIII	PC ID	
			(All versions), SIMATIC HM	II				
			KTP Mobile Panels KTP400	F,				
			KTP700, KTP700F, KTP900)				
			und KTP900F (All versions),				
			SIMATIC IPC DiagMonitor					
			(All versions), SIMATIC					
			RF181-EIP (All versions),					
			SIMATIC RF182C (All					
			versions), SIMATIC RF1860	G				
			(All versions), SIMATIC					
			RF188C (All versions),					
			SIMATIC RF600R (All					
			versions), SIMATIC S7-150	0				
			CPU family (All versions),					
			SIMATIC S7-1500 Software	2				
			Controller (All versions),					
			SIMATIC S7-300 CPU famil	v				
	(All versions							
		SIMATIC S7-400 PN (incl. F	n l					
			V6 and below (All versions),					
			SIMATIC S7-400 PN/DP V7					
			(incl. F) (All versions),					
			SIMATIC S7-PLCSIM					
			Advanced (All versions),					
			SIMATIC Teleservice					
			Adapter IE Advanced (All					
			versions), SIMATIC	<u>.</u> .				
			Teleservice Adapter IE Bas	1C				
			(All versions), SIMATIC					
			Teleservice Adapter IE					
			Standard (All versions),					
			SIMATIC WinAC RTX 2010					
			(All versions), SIMATIC					
			WinCC Runtime Advanced					
			(All versions), SIMOCODE					
			pro V EIP (All versions),					
			SIMOCODE pro V PN (All					
			versions), SINAMICS G130					
			V4.6 (All versions),					
CV Scoring Sca	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10	
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	0-7	7-0	0-9	3-10	

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIIF	PC ID	
			SINAN	AICS G1:	30 V4.7	(All					
					AMICS (`					
			V4.7 S	SP1 (All	versions	;),					
			SINAN	AICS G1	30 V4.8	(All					
			versions < V4.8 HF6),								
			SINAN	MICS G1	30 V5.1	(All					
			versio	ns), SIN	AMICS (G130					
			V5.1 S	SP1 (All	versions	< V5.1					
			SP1 H	F4), SIN	AMICS (G150					
			V4.6 (All vers	ions),						
			SINAN	MICS G1	50 V4.7	(All					
			versio	ns), SIN	AMICS (G150					
			V4.7 S	SP1 (All	versions	;),					
			SINAN	AICS G1	50 V4.8	(All					
				ns < V4							
			SINAN	MICS G1	50 V5.1	(All					
			versio	ns), SIN	AMICS (G150					
					versions						
			SP1 H	F4), SIN	AMICS S	5120					
			V4.6 (All vers	ions),						
			SINAN	MICS S12	20 V4.7 ([All					
			versio	ns), SIN	AMICS S	5120					
			V4.7 S	SP1 (All	versions	;),					
				-	20 V4.8 (-					
			versio	ns < V4	.8 HF6),	-					
			SINAN	AICS S12	20 V5.1 (All					
			versio	ns), SIN	AMICS S	S120					
				-	versions						
				•	AMICS S						
				All vers							
			`		50 V4.7 (All					
					AMICS S	•					
				-							
			V4.7 SP1 (All versions), SINAMICS S150 V4.8 (All								
				ns < V4							
			SINAMICS S150 V5.1 (All								
					AMICS S	•					
				-	versions						
				-	AMICS S						
CV Scoring Sca	le			-							
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1	

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	IPC ID
			SINAN (All ve Mana) SITOF versice (All ve (All ve webse device vulne to a d condi cause situat restar the af secur be exp with r affect explo syster user i could to cor the de advise public	evice. At ory publ c exploit ity vulne	to V5.1; SITOP versions 00 (All OP UPS; TIM 15 The the affectins a that may eservice attacker ch leads webserv evice. Tl erability by an att access t ms. Success equires eges and on. An a vulnera the time ication of	s), 1600 31 IRC cted y lead r may rice to a rer of he could acker to the cessful no no ttacker bility bility of e of no this				
			CVE I	D : CVE-	2019-6	568				
simatic_s7-15	00f_firmwai	e								
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC				II N/A			-SIMA- 19/443
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
[CV.3.3]										

Vulnerability Type(s)	Publish Date	cvss	D	escriptio	n & CVE	ID	Pa	tch	NCIII	PC ID
			CP343-	-1 Advai	nced (A	11				
				ns), SIM						
			(All vei	rsions),	SIMATI	С				
			-	-1 Advai						
				ns), SIM	•					
				A (All ve						
				IC ET 20	,					
				ller CPU	_					
			(All vei	rsions <	V2.1.6)	,				
			-	IC ET 20	-					
				ller CPU						
				rsions),						
			`	rt Outdo						
				l versio						
			`	mfort P						
				rsions),						
			`	obile Pa						
				0, KTP7						
				'P900F (
				IC IPC D	•					
				rsions),	•					
			`	-EIP (All						
				IC RF18		113),				
				ic id 10 is), SIM <i>i</i>	•	1960				
				-						
			-	rsions), :						
				C (All ve	_	,				
				IC RF60	•	1500				
				rs), SIMA						
				mily (All		-				
				IC S7-15						
				ller (All		· .				
				IC S7-30						
			`	rsions <						
				IC S7-40	•	•				
				below (•	-				
				IC S7-40	•					
	(incl. F) (All version				-					
			SIMATIC S7-PLCSIM							
			Advanced (All versions),							
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	De	escription & CV	E ID	Pa	tch	NCIII	PC ID
			SIMATI	C Teleservice	<u> </u>				
			Adapte	r IE Advance	l (All				
			version	s), SIMATIC					
			Teleser	vice Adapter	IE Basic				
				rsions), SIMA'					
			`	vice Adapter					
				rd (All versio					
			SIMATI	C WinAC RTX	2010				
			(All ver	rsions), SIMA'	ГІС				
			`	Runtime Adv					
			(All ver	sions), SIMO	CODE				
			_	IP (All versio					
			•	DDE pro V PN	-				
				s), SINAMICS	-				
				ll versions),	G100				
			`	ICS G130 V4.7	7 (All				
				s), SINAMICS	•				
				1 (All version					
				ICS G130 V4.8					
				s < V4.8 HF6	•				
				ICS G130 V5.1					
				ics d130 v3 is), SINAMICS	•				
				13), SinAmics 1 (All version					
				4), SINAMICS					
					G130				
			-	ll versions),	7 (
				ICS G150 V4.7					
				s), SINAMICS					
				1 (All version					
				ICS G150 V4.8	•				
				s < V4.8 HF6					
				ICS G150 V5.2					
				s), SINAMICS					
				1 (All version					
				4), SINAMICS	S120				
			V4.6 (A	ll versions),					
				ICS S120 V4.7					
				s), SINAMICS					
		V4.7 SP1 (All versions),							
		SINAMICS S120 V4.8 (All							
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE	ID	Pat	tch	NCIII	PC ID
			versions < V	l.8 HF6),					
			SINAMICS S1	20 V5.1 (All				
			versions), SII	NAMICS S	120				
			V5.1 SP1 (All	versions	< V5.1				
			SP1 HF4), SII	NAMICS S	150				
			V4.6 (All ver	sions),					
			SINAMICS S1	50 V4.7 (All				
			versions), SII	NAMICS S	150				
			V4.7 SP1 (All	versions),				
			SINAMICS S1	50 V4.8 (All				
			versions < V	l.8 HF6),					
			SINAMICS S1	50 V5.1 (All				
			versions), SII	NAMICS S	150				
			V5.1 SP1 (All	versions	< V5.1				
			SP1 HF4), SII	NAMICS S	210				
			V5.1 (All ver	sions),					
			SINAMICS S2	10 V5.1 S	SP1				
			(All versions), SITOP					
			Manager (All	versions),				
			SITOP PSU86	600 (All					
			versions), SI	TOP UPS1	.600				
			(All versions), TIM 15	31 IRC				
			(All versions). The					
			webserver of	the affec	ted				
			devices conta	ains a					
			vulnerability	that may	lead				
			to a denial-o	-service					
			condition. Ar	attacker	may				
			cause a denia	ıl-of-serv	ice				
			situation wh	ch leads	to a				
			restart of the	webserv	er of				
			the affected o	levice. Th	ie				
			security vuln	erability	could				
			be exploited	by an atta	acker				
			with networl	k access t	o the				
			affected syste	ems. Succ	essful				
			exploitation	requires	10				
			system privil	eges and	no				
			user interact	ion. An at	tacker				
CV Scoring Scal	e 0.1	1-2	2.3 2.4	<i>1</i> E	5 G	6.7	7.0	9.0	0.10
(CVSS)	0-1 pe(s): CSRF- Cross	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6568		
Improper Input Validation	17-04-2019	7.8	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP PC2 (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC NET PC Software (All versions), SIMATIC RF188C (All versions), SIMATIC RF600R (All versions), SIMATIC S7-1500 CPU family (All versions >= V2.5), SIMATIC S7-1500 Software Controller (All versions >= V2.5), SIMATIC WinCC OA (All versions < V3.15-P018), SIMATIC WinCC Runtime Advanced (All versions), SIMATIC WinCC Runtime Comfort (All versions), SIMATIC WinCC Runtime HSP Comfort (All versions), SINECNMS (All versions), SINEMA Server (All versions), SINEMA Server (All versions), SINEMA Server (All versions), SINUMERIK OPC UA Server (All versions < V2.1),	N/A	O-SIE-SIMA- 010519/444

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

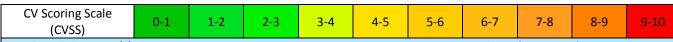
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; Dos-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			version network affects with a track service comments of the control of the control of the control of the control of the time publice exploration of the control of the time publice exploration of the control of the time time of the control of the of the co	ork accesed syste itation reprivite merivite merivite use the	ecially creets sent es on pold allow ted remouse a Decinity could be an attacked an attacked equires eges and on. An avulneration of this se was known as kn	rafted to ort an ote enial-of- he OPC ash the cessful no no ttacker bility bility of on. At curity wn.				
simatic_s7-15	00s_firmwar	e							_	
Improper Input Validation	17-04-2019	5	identi versic (All ve CP343 versic (All ve CP443 versic OPC U	nerabilit ified in C ons), CP1 ons), SIA ersions) 3-1 Adva ons), SIM ons), SIM JA (All v	EP1604 (Al MTIC RI , SIMAT) anced (A IATIC CI , SIMAT) anced (A IATIC CI ersions)	(All ll F185C IC All P443-1 IC All	N/A			SIMA- 9/445
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 Typ	pe(s): CSRF- Cross Denial of Service	_				_				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE I	D	Pa	tch	NCII	PC ID
			Controller CI	U 1515SF	PC				
			(All versions	< V2.1.6),					
			SIMATIC ET	200 SP Op	en				
			Controller CI	PU 1515SF	PC2				
			(All versions), SIMATIO	CHMI				
			Comfort Out	door Pane	ls 7" &				
			15" (All versi	ons), SIM	ATIC				
			HMI Comfort	Panels 4"	- 22"				
			(All versions), SIMATIO	CHMI				
			KTP Mobile I	anels KTI	P400F,				
			KTP700, KTF	700F, KT	P900				
			und KTP900	F (All vers	ions),				
			SIMATIC IPC	-					
			(All versions	•					
			RF181-EIP (A						
			SIMATIC RF1		- 57				
			versions), SII	•	186C				
			(All versions						
			RF188C (All						
			SIMATIC RF6	-					
			versions), SII	-	1500				
			CPU family (A						
			SIMATIC S7-		-				
			Controller (A						
			SIMATIC S7-		-				
			(All versions		-				
			SIMATIC S7-		· .				
			V6 and below	•	_				
			SIMATIC S7-	•					
			(incl. F) (All v	•	r v /				
				,					
			SIMATIC S7-						
			Advanced (A		iJ,				
			SIMATIC Tele		A 11				
			Adapter IE A						
			versions), SII						
			Teleservice A						
	(All versions), SIM Teleservice Adapt								
				•					
				Standard (All versions),					
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross								

Vulnerability Type(s)	Publish Date	cvss	Descripti	on & CVE	ID	Pat	tch	NCIII	PC ID
			SIMATIC Win	AC RTX 2	2010				
			(All versions)	, SIMATI	C				
			WinCC Runtii	ne Advai	nced				
			(All versions)	, SIMOCO	DDE				
			pro V EIP (All	version	s),				
	SIMOCODE pro V PN (All								
			versions), SIN	IAMICS (G130				
			V4.6 (All vers	ions),					
			SINAMICS G1	30 V4.7 ((All				
			versions), SIN	IAMICS (G130				
			V4.7 SP1 (All	versions),				
			SINAMICS G1	30 V4.8 (All				
			versions < V4		•				
			SINAMICS G1	· ·	All				
			versions), SIN						
			V5.1 SP1 (All						
			SP1 HF4), SIN						
			V4.6 (All vers		.100				
			SINAMICS G1	-	(All				
			versions), SIN		•				
			V4.7 SP1 (All						
			SINAMICS G1		-				
			versions < V4		[7111				
			SINAMICS G1	-	Δ11				
					-				
			versions), SIN						
			V5.1 SP1 (All						
			SP1 HF4), SIN		120				
			V4.6 (All vers	-	· A 11				
			SINAMICS S1	`	•				
			versions), SIN						
			V4.7 SP1 (All		-				
			SINAMICS S1	`	All				
			versions < V4	,					
			SINAMICS S1	`	•				
			versions), SIN						
			V5.1 SP1 (All						
			SP1 HF4), SINAMICS S150						
			V4.6 (All vers	-					
			SINAMICS S1	50 V4.7 (All				
CV Scoring Sca	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0 1		2 3 4	7 3	3 0	0 /	, 0	0 9	J 1

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			versions), SINAMICS S150		
			V4.7 SP1 (All versions),		
			SINAMICS S150 V4.8 (All		
			versions < V4.8 HF6),		
			SINAMICS S150 V5.1 (All		
			versions), SINAMICS S150		
			V5.1 SP1 (All versions < V5.1		
			SP1 HF4), SINAMICS S210		
			V5.1 (All versions),		
			SINAMICS S210 V5.1 SP1		
			(All versions), SITOP		
			Manager (All versions),		
			SITOP PSU8600 (All		
			versions), SITOP UPS1600		
			(All versions), TIM 1531 IRC		
			(All versions). The		
			webserver of the affected		
			devices contains a		
			vulnerability that may lead		
			to a denial-of-service		
			condition. An attacker may		
			cause a denial-of-service		
			situation which leads to a		
			restart of the webserver of		
			the affected device. The		
			security vulnerability could		
			be exploited by an attacker		
			with network access to the		
			affected systems. Successful		
			exploitation requires no		
			system privileges and no		
			user interaction. An attacker		
			could use the vulnerability		
			to compromise availability of		
			the device. At the time of		
			advisory publication no		
			public exploitation of this		
			security vulnerability was		



Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			known. CVE ID : CVE-2019-6568		
Improper Input Validation	17-04-2019	7.8	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP PC2 (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC NET PC Software (All versions), SIMATIC RF188C (All versions), SIMATIC RF600R (All versions), SIMATIC S7-1500 CPU family (All versions >= V2.5), SIMATIC S7-1500 Software Controller (All versions >= V2.5), SIMATIC WinCC OA (All versions < V3.15-P018), SIMATIC WinCC Runtime Advanced (All versions), SIMATIC WinCC Runtime Comfort (All versions), SIMATIC WinCC Runtime HSP Comfort (All versions), SIMATIC WinCC Runtime HSP Comfort (All versions), SIMATIC WinCC Runtime HSP Comfort (All versions), SINECNMS (All versions), SINECNMS (All versions), SINECNMS (All versions), SINEMA Server (All versions), SINEMA Server (All versions), SINUMERIK OPC UA Server (All versions). Specially crafted network packets sent to affected devices on port 4840/tcp could allow an unauthenticated remote	N/A	O-SIE-SIMA- 010519/446

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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; Dos-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			Service commended device vulne explored affect explored affect explored affect explored device could to conthe Office the time publice explored vulne explored affect explored	ork accested syste itation rule interaction use the impromise PC comments of addition or ability	tion of the on or crace curity could be an attack as to the ms. Succeedings and on. An acceeding a vulneraction of this seems was known as the country of this seems as the country of t	ne OPC ash the exer with cessful no no ttacker bility bility of on. At curity wn.				
simatic_s7-15	00t firmwar	P	CVEI	D : CVE-	2019-6	575				
Improper Input Validation	17-04-2019	5	identi versic (All versic (All versic (All versic (All versic OPC U SIMA' Contr (All versic	nerabilit fied in C ons), CP1 ons), SIA ersions) 3-1 Adva ons), SIM ersions) G-1 Adva ons), SIM CF ET 2 oller CP ersions oller CP ersions) ort Outd	EP1604 (Al Al A	[All I	N/A			SIMA- 9/447
CV Scoring Sca	Θ.	1-2	2-3				6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descripti	on & CVE ID		Pa	tch	NCIII	PC ID
			15" (All versi	ons), SIMA	TIC				
			HMI Comfort	Panels 4"	- 22"				
			(All versions)	, SIMATIC	HMI				
			KTP Mobile P	anels KTP	400F,				
			KTP700, KTP						
			und KTP900F						
			SIMATIC IPC	•	٠.				
			(All versions)	_					
			RF181-EIP (A						
			SIMATIC RF1		,				
			versions), SIN	•	86C				
			(All versions)						
			RF188C (All v						
			SIMATIC RF6	-					
			versions), SIN	•	1500				
			CPU family (A						
			SIMATIC S7-1		-				
			Controller (A						
			SIMATIC S7-3						
					-				
			(All versions	-					
			SIMATIC S7-4	•	_				
			V6 and below	-	_				
			SIMATIC S7-4	-	, , ,				
			(incl. F) (All v	_					
			SIMATIC S7-F						
			Advanced (Al	_),				
			SIMATIC Tele						
			Adapter IE Ad	•	All				
			versions), SIN	IATIC					
			Teleservice A	dapter IE	Basic				
			(All versions)	, SIMATIC					
			Teleservice A	dapter IE					
			Standard (All	versions),	,				
			SIMATIC Win	AC RTX 20	010				
			(All versions)	, SIMATIC					
			WinCC Runtii	ced					
			(All versions)						
			pro V EIP (All						
			SIMOCODE pi	-					
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	0.1
(CVSS)	0-1	1-2	2-3 3-4	4-5	3-0	0-7	7-0	0-3	9-1

Vulnerability Type(s)	Publish Date	cvss	Description & CV	E ID P	atch	NCIII	PC ID
			versions), SINAMICS	G130			
			V4.6 (All versions),				
			SINAMICS G130 V4.7	' (All			
			versions), SINAMICS	G130			
			V4.7 SP1 (All version	ıs),			
			SINAMICS G130 V4.8	B (All			
			versions < V4.8 HF6	,			
			SINAMICS G130 V5.1	(All			
			versions), SINAMICS	G130			
			V5.1 SP1 (All version	ıs < V5.1			
			SP1 HF4), SINAMICS	G150			
			V4.6 (All versions),				
			SINAMICS G150 V4.7	' (All			
			versions), SINAMICS	`			
			V4.7 SP1 (All version				
			SINAMICS G150 V4.8	·			
			versions < V4.8 HF6	•			
			SINAMICS G150 V5.1				
			versions), SINAMICS	`			
			V5.1 SP1 (All version				
			SP1 HF4), SINAMICS				
			V4.6 (All versions),	5120			
			SINAMICS S120 V4.7	(All			
			versions), SINAMICS	`			
			V4.7 SP1 (All version				
			SINAMICS S120 V4.8	·			
			versions < V4.8 HF6	`			
			SINAMICS S120 V5.1				
			versions), SINAMICS	`			
			V5.1 SP1 (All version				
			-				
			SP1 HF4), SINAMICS	3150			
			V4.6 (All versions),	CALL			
			SINAMICS S150 V4.7	•			
			versions), SINAMICS				
			V4.7 SP1 (All version	•			
			SINAMICS S150 V4.8	•			
			versions < V4.8 HF6				
			SINAMICS S150 V5.1	`			
			versions), SINAMICS	5150			
CV Scoring Sca	0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross	C'I D					

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			V5.1 SP1 (All versions < V5.1 SP1 HF4), SINAMICS S210 V5.1 (All versions), SINAMICS S210 V5.1 SP1 (All versions), SITOP Manager (All versions), SITOP PSU8600 (All versions), SITOP UPS1600 (All versions), TIM 1531 IRC (All versions). The webserver of the affected devices contains a vulnerability that may lead to a denial-of-service condition. An attacker may cause a denial-of-service situation which leads to a restart of the webserver of the affected device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.		
Improper			CVE ID : CVE-2019-6568 A vulnerability has been		
Improper Input Validation	17-04-2019	7.8	identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200	N/A	0-SIE-SIMA- 010519/448

0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

CV Scoring Scale

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	tch	NCIII	PC ID
			Open Controller CPU 151	15SP			
			PC2 (All versions), SIMA'	TIC			
			IPC DiagMonitor (All				
			versions), SIMATIC NET	PC			
			Software (All versions),				
			SIMATIC RF188C (All				
			versions), SIMATIC RF60	00R			
			(All versions), SIMATIC S	57-			
			1500 CPU family (All				
			versions >= V2.5), SIMAT	ГІС			
			S7-1500 Software Contro	oller			
			(All versions >= V2.5),				
			SIMATIC WinCC OA (All				
			versions < V3.15-P018),				
			SIMATIC WinCC Runtime	e			
			Advanced (All versions),				
			SIMATIC WinCC Runtime				
			Comfort (All versions),				
			SIMATIC WinCC Runtime	Δ			
			HSP Comfort (All version				
			SIMATIC WinCC Runtime	•			
			Mobile (All versions), SIN				
			NMS (All versions), SINE				
			Server (All versions),	IVIA			
			SINUMERIK OPC UA Serv	ior			
				vei			
			(All versions < V2.1),	. (11			
			TeleControl Server Basic	`			
			versions). Specially craft	ea			
			network packets sent to				
			affected devices on port				
			4840/tcp could allow an				
			unauthenticated remote				
			attacker to cause a Denia				
			Service condition of the (
			communication or crash	the			
			device. The security				
			vulnerability could be				
			exploited by an attacker with				
			network access to the				
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty	0-1	1 2	2-9 3-4 4-3	3 0 0-7	7-0	3-9	J-10

Vulnerability Type(s)	Publish Date	cvss	I	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			explo syster user i could to cor the Of the tin public explo vulne	ed syste itation renderaction use the mpromise PC comments attion to the itation of additation of a distinguishing the control of the control	equires eges and on. An a vulnera e availa nunicati visory o public f this se was kno	no ttacker bility bility of on. At curity				
simatic_s7-30	0_firmware									
Improper Input Validation	17-04-2019	5	identi versic (All versic (All versic (All versic (All versic OPC U SIMA' Contr (All versic Contr (All versic (All	nerabilited in Cons), CP2 ons), SIA ersions) 3-1 Adva ons), SIM ersions) 3-1 Adva ons), SIM JA (All v TIC ET 2 oller CP ersions ort Outd All versio Comfort ersions) Mobile P TIC IPC I	P1604 (All MTIC RIATIC RIATIC CIESTONS) OU 15155 V2.1.6 OU 51555 V2.1.6 OU 51555 V2.1.6 OU 75155 V2.1.6 OU 751	(All ll ll F185C IC ll P443-1 IC ll P443-1 l, pen SP PC l), pen SP PC2 IC HMI els 7" & MATIC ll HMI CP400F, FP900 rsions),	N/A			-SIMA- 19/449
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	pe(s): CSRF- Cross Denial of Service	_				_				on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	:ch	NCIII	PCID
			(All versions), SIMATIC				
			RF181-EIP (All versions),				
			SIMATIC RF182C (All				
			versions), SIMATIC RF186	SC			
			(All versions), SIMATIC				
			RF188C (All versions),				
			SIMATIC RF600R (All				
			versions), SIMATIC S7-15	00			
			CPU family (All versions),				
			SIMATIC S7-1500 Softwar	·e			
			Controller (All versions),				
			SIMATIC S7-300 CPU fami	lv			
			(All versions < V3.X.16),	9			
			SIMATIC S7-400 PN (incl.	F)			
			V6 and below (All version	-			
			SIMATIC S7-400 PN/DP V				
			(incl. F) (All versions),	'			
			SIMATIC S7-PLCSIM				
			Advanced (All versions),				
			SIMATIC Teleservice				
			Adapter IE Advanced (All				
			versions), SIMATIC				
			Teleservice Adapter IE Ba	SIC			
			(All versions), SIMATIC				
			Teleservice Adapter IE				
			Standard (All versions),				
			SIMATIC WinAC RTX 2010)			
			(All versions), SIMATIC				
			WinCC Runtime Advanced	l			
			(All versions), SIMOCODE				
			pro V EIP (All versions),				
			SIMOCODE pro V PN (All				
			versions), SINAMICS G130)			
			V4.6 (All versions),				
			SINAMICS G130 V4.7 (All				
			versions), SINAMICS G130)			
			V4.7 SP1 (All versions),				
			SINAMICS G130 V4.8 (All				
			versions < V4.8 HF6),				
CV Scoring Sca	e 0.1	1.2	22 24 45 5	6 67	7.0	9.0	0.1
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-	6 6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			SINAN	AICS G1	30 V5.1	(All				
					AMICS (•				
				-	versions					
				•	AMICS (
				All vers						
			`	•	50 V4.7	(All				
					AMICS (•				
				-	versions					
				•	50 V4.8					
					.8 HF6),	•				
					50 V5.1					
					AMICS (•				
					versions					
				•	AMICS S					
				All vers						
			`		20 V4.7	All				
					AMICS S	-				
				-	versions					
				•	20 V4.8					
					.8 HF6),					
					20 V5.1	All				
					AMICS S	•				
				-	versions					
				•	AMICS S					
				All vers						
			7		50 V4.7	All				
					AMICS S	•				
				-	versions					
				•	50 V4.8	-				
					.8 HF6),	(
					50 V5.1	All				
					AMICS S	-				
					versions					
				•						
			SP1 HF4), SINAMICS S210 V5.1 (All versions), SINAMICS S210 V5.1 SP1							
			(All versions), SITOP							
					Manager (All versions),					
			SITOP PSU8600 (All							
CV Scoring Sca	le la				-					
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			versions), SITOP UPS1600 (All versions), TIM 1531 IRC (All versions). The webserver of the affected devices contains a vulnerability that may lead to a denial-of-service condition. An attacker may cause a denial-of-service situation which leads to a restart of the webserver of the affected device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6568		
simatic_s7-40	0_pn/dp_firm	ware			
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 Advanced (All versions), SIMATIC CP443-1 SIMATIC CP443-1	N/A	O-SIE-SIMA- 010519/450
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7	7-8 8-9 9-10
		_	uest Forgery; Dir. Trav Directory Trav oss Site Scripting; Sql- SQL Injection; N		

Vulnerability Type(s)	Publish Date	cvss	Description & C	/E ID	Patch	NCIII	PCID
			OPC UA (All version	s),			
			SIMATIC ET 200 SF	Open			
			Controller CPU 151	5SP PC			
			(All versions < V2.1	.6),			
			SIMATIC ET 200 SF	Open			
			Controller CPU 151	5SP PC2			
			(All versions), SIMA	TIC HMI			
			Comfort Outdoor P	nnels 7" &			
			15" (All versions), S	IMATIC			
			HMI Comfort Panel	s 4" - 22"			
			(All versions), SIMA	TIC HMI			
			KTP Mobile Panels				
			KTP700, KTP700F,	·			
			und KTP900F (All v				
			SIMATIC IPC DiagM	٠.			
			(All versions), SIMA				
			RF181-EIP (All ver				
			SIMATIC RF182C (A	•			
			versions), SIMATIC				
			(All versions), SIMA				
			RF188C (All version				
			SIMATIC RF600R (-			
			versions), SIMATIC				
			CPU family (All ver				
			SIMATIC S7-1500 S	· .			
			Controller (All vers	-			
			SIMATIC S7-300 CF	-			
			(All versions < V3.X	-			
			SIMATIC S7-400 PN	,			
			V6 and below (All v	,			
			SIMATIC S7-400 PN				
			(incl. F) (All version	•			
			SIMATIC S7-PLCSIN				
			Advanced (All vers	-			
	SIMATIC Telesery			e			
			Adapter IE Advance	d (All			
			versions), SIMATIC				
			Teleservice Adapte	· IE Basic			
			(All versions), SIMA	TIC			
CV Scoring Sca	e	1.2	2.2	E.C. C.	7 7 0	0.0	0.4
(CVSS)	0-1	1-2	2-3 3-4 4-5	5-6 6-1	7 7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	tch	NCIII	PC ID
			Teleservice Adapter IE				
			Standard (All versions),				
			SIMATIC WinAC RTX 20	10			
			(All versions), SIMATIC				
			WinCC Runtime Advanc	ed			
			(All versions), SIMOCOI)E			
			pro V EIP (All versions)	,			
			SIMOCODE pro V PN (A)	11			
			versions), SINAMICS G1	30			
			V4.6 (All versions),				
			SINAMICS G130 V4.7 (A	11			
			versions), SINAMICS G1	30			
			V4.7 SP1 (All versions),				
			SINAMICS G130 V4.8 (A	11			
			versions < V4.8 HF6),				
			SINAMICS G130 V5.1 (A	11			
			versions), SINAMICS G1	30			
			V5.1 SP1 (All versions <	V5.1			
			SP1 HF4), SINAMICS G1	50			
			V4.6 (All versions),				
			SINAMICS G150 V4.7 (A	11			
			versions), SINAMICS G1	50			
			V4.7 SP1 (All versions),				
			SINAMICS G150 V4.8 (A	11			
			versions < V4.8 HF6),				
			SINAMICS G150 V5.1 (A	11			
			versions), SINAMICS G1				
			V5.1 SP1 (All versions <				
			SP1 HF4), SINAMICS S1				
			V4.6 (All versions),				
			SINAMICS S120 V4.7 (A	11			
			versions), SINAMICS S1				
			V4.7 SP1 (All versions),				
			SINAMICS S120 V4.8 (A	n			
			versions < V4.8 HF6),	·•			
			SINAMICS S120 V5.1 (A	₁₁			
		versions), SINAMICS S120					
			V5.1 SP1 (All versions <				
			SP1 HF4), SINAMICS S1				
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty							

Vulnerability Type(s)	Publish Date	cvss	Des	scription & CVE	ID	Pat	tch	NCIII	PC ID
			V4.6 (Al	l versions),					
			SINAMI	CS S150 V4.7 (All				
			versions	s), SINAMICS S	5150				
			V4.7 SP1	l (All versions),				
			SINAMI	CS S150 V4.8 (All				
			versions	s < V4.8 HF6),					
			SINAMI	CS S150 V5.1 (All				
			versions	s), SINAMICS S	5150				
			V5.1 SP1	l (All versions	< V5.1				
			SP1 HF4), SINAMICS S	210				
			V5.1 (Al	l versions),					
			SINAMI	CS S210 V5.1 S	SP1				
			-	sions), SITOP					
			Manage	r (All versions),				
			SITOP P	SU8600 (All					
			versions	s), SITOP UPS1	.600				
			(All vers	ions), TIM 15	31 IRC				
			`	sions). The					
			webserv	er of the affec	ted				
			devices	contains a					
				oility that may	lead				
			to a den	ial-of-service					
			conditio	n. An attacker	may				
			cause a	denial-of-serv	ice				
			situatio	n which leads	to a				
			restart o	of the webserv	er of				
			the affec	ted device. Th	ie				
			security	vulnerability	could				
			be explo	ited by an atta	acker				
			with net	work access t	o the				
			affected	systems. Succ	essful				
			exploita	tion requires	no				
			system p	orivileges and	no				
			user inte	eraction. An at	tacker				
			could us	e the vulneral	oility				
			to compromise availability of						
			the devi	ce. At the time	e of				
			advisory	publication r	10				
			public e	xploitation of	this				
CV Scoring Scal	e 0-1	1-2	2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	pe(s): CSRF- Cross								

Vulnerability Type(s)	Publish Date	cvss	•	Description	on & CVE	ID	Pa	itch	NCII	PC ID
			know	ity vulne n. D : CVE-	-					
simatic_s7-40	0_pn_firmwa	re								
Improper Input Validation	17-04-2019	5	identi versic (All ve CP343 versic (All ve CP443 versic OPC U SIMA' Contr (All ve SIMA' Contr (All ve KTP N KTP7 und K SIMA' (All ve RF183 SIMA' versic (All ve RF183 SIMA' versic	nerability fied in Cons), CP1 ons), SIA ersions), 3-1 Adva ons), SIM ersions), 3-1 Adva ons), SIM JA (All versions), ort Outd All versions), ort Outd	P1604 (Ale Called Calle	(All II I	N/A			SIMA- 9/451
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 Typ	pe(s): CSRF- Cross Denial of Service	_				_			ntormatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	-	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			SIMA	ΓΙC S7-1	500 Sof	tware				
			Contr	oller (Al	l version	1s),				
			SIMA	ΓΙC S7-3	00 CPU	family				
				ersions <		-				
			SIMA	ΓIC S7-4	00 PN (i	ncl. F)				
			V6 an	d below	(All ver	sions),				
			SIMA	ΓIC S7-4	00 PN/I	OP V7				
			(incl.	F) (All v	ersions)	,				
			SIMA	ΓIC S7-P	LCSIM					
			Advar	nced (All	version	ıs),				
			SIMA	ΓIC Tele	service					
			Adapt	er IE Ad	vanced	(All				
			versio	ns), SIM	IATIC					
			Telese	ervice A	dapter II	E Basic				
			(All ve	ersions)	, SIMATI	C				
			Telese	ervice A	dapter II	Е				
			Stand	ard (All	versions	s),				
			SIMA	ΓIC Win.	AC RTX	2010				
			(All ve	ersions)	, SIMATI	(C				
			WinC	C Runtin	ne Adva	nced				
			(All ve	ersions)	SIMOC	ODE				
			pro V	EIP (All	version	s),				
			SIMO	CODE pr	o V PN (All				
			versio	ns), SIN	AMICS (G130				
			V4.6 (All vers	ions),					
			SINAN	MICS G1	30 V4.7	(All				
			versio	ns), SIN	AMICS (G130				
			V4.7 S	SP1 (All	versions	s),				
			SINAN	MICS G1	30 V4.8	(All				
			versio	ns < V4	.8 HF6),					
			SINAN	MICS G1	30 V5.1	(All				
			versio	ns), SIN	AMICS (G130				
			V5.1 S	SP1 (All	versions	s < V5.1				
			SP1 H	F4), SIN	AMICS (G150				
			V4.6 (V4.6 (All versions),						
			SINAMICS G150 V4.7 (All							
			versions), SINAMICS G150							
				V4.7 SP1 (All versions),						
			SINAN	MICS G1	50 V4.8	(All				
CV Scoring Sca	le 0.1	1_2	2.2	2 /	<i>/</i> [E 6	6.7	7 0	9.0	0.1
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patc	h	NCIII	PC ID
			versions < V4.8 HF6),				
			SINAMICS G150 V5.1 (All				
			versions), SINAMICS G150				
			V5.1 SP1 (All versions < V5.	1			
			SP1 HF4), SINAMICS S120				
			V4.6 (All versions),				
			SINAMICS S120 V4.7 (All				
			versions), SINAMICS S120				
			V4.7 SP1 (All versions),				
			SINAMICS S120 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S120 V5.1 (All				
			versions), SINAMICS S120				
			V5.1 SP1 (All versions < V5.	1			
			SP1 HF4), SINAMICS S150				
			V4.6 (All versions),				
			SINAMICS S150 V4.7 (All				
			versions), SINAMICS S150				
			V4.7 SP1 (All versions),				
			SINAMICS S150 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S150 V5.1 (All				
			versions), SINAMICS S150				
			V5.1 SP1 (All versions < V5.	1			
			SP1 HF4), SINAMICS S210				
			V5.1 (All versions),				
			SINAMICS S210 V5.1 SP1				
			(All versions), SITOP				
			Manager (All versions),				
			SITOP PSU8600 (All				
			versions), SITOP UPS1600				
			(All versions), TIM 1531 IR	,			
			(All versions). The				
			webserver of the affected				
			devices contains a				
			vulnerability that may lead				
			to a denial-of-service				
			condition. An attacker may cause a denial-of-service				
CV Scoring Scal	e e	4.0			7.0		
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	I	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			restar the af securi be exp with raffect explo syster user i could to cor the de advise public securi know	evice. At ory publ c exploit ity vulne	webserverice. The rability of an attended access to the sequires of availation of erability	ver of he could acker to the cessful no no ttacker bility bility of e of no this was				
simatic_rf188	c_firmware									
Improper Input Validation	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All versions), SIAMTIC RF185C (All versions), SIMATIC CP343-1 Advanced (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2 (All versions), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions), SIMATIC				N/A			SIMA- 9/452
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 Typ	pe(s): CSRF- Cross Denial of Service	_				_			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patc	h	NCIIP	PC ID			
			HMI Comfort Panels 4" - 22	2"						
			(All versions), SIMATIC HN	ΛI						
			KTP Mobile Panels KTP400	OF,						
			KTP700, KTP700F, KTP900							
			und KTP900F (All versions	s),						
			SIMATIC IPC DiagMonitor							
			(All versions), SIMATIC							
			RF181-EIP (All versions),							
			SIMATIC RF182C (All							
			versions), SIMATIC RF186	С						
			(All versions), SIMATIC							
			RF188C (All versions),							
			SIMATIC RF600R (All							
			versions), SIMATIC S7-150	00						
			CPU family (All versions),							
			SIMATIC S7-1500 Softwar	e l						
			Controller (All versions),							
			SIMATIC S7-300 CPU famil	lv						
			(All versions < V3.X.16),	ay						
			SIMATIC S7-400 PN (incl. l	E)						
			V6 and below (All versions	-						
			SIMATIC S7-400 PN/DP V							
			·	'						
			(incl. F) (All versions),							
			SIMATIC S7-PLCSIM							
			Advanced (All versions),							
			SIMATIC Teleservice							
			Adapter IE Advanced (All							
			versions), SIMATIC							
			Teleservice Adapter IE Bas	sic						
			(All versions), SIMATIC							
			Teleservice Adapter IE							
			Standard (All versions),							
			SIMATIC WinAC RTX 2010)						
			(All versions), SIMATIC							
			WinCC Runtime Advanced							
			(All versions), SIMOCODE							
			pro V EIP (All versions),							
			SIMOCODE pro V PN (All							
			versions), SINAMICS G130							
CV Scoring Scal	e	1.3	2.2 2.4 4.5 5.4	6 67	7.0	0.0	0.4			
(CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10			

Vulnerability Type(s)	Publish Date	cvss		Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			V4.6 (All vers	ions),					
			SINA	MICS G1	30 V4.7	(All				
			versio	ns), SIN	AMICS (G130				
			V4.7 S	SP1 (All	versions	s),				
			SINA	MICS G1	30 V4.8	(All				
			versio	ons < V4	.8 HF6),					
			SINA	MICS G1	30 V5.1	(All				
			versio	ons), SIN	AMICS (G130				
			V5.1 S	SP1 (All	versions	s < V5.1				
		G150								
			V4.6 (All vers	ions),					
			· ·	MICS G1	-	(All				
				ons), SIN		•				
				SP1 (All						
				MICS G1						
				ons < V4		•				
				MICS G1	-					
				ons), SIN		•				
				SP1 (All						
				1F4), SIN						
				All vers		71_0				
			1	MICS S12	_	(All				
				ons), SIN						
				SP1 (All						
				MICS S12		,				
				ons < V4		(7111				
				MICS S12	-	(A))				
				ns), SIN		•				
				SP1 (All						
				151 (A11 154), SIN						
				All vers		3130				
			•	MICS S15		(A 11				
						-				
				ons), SIN						
				SP1 (All						
				MICS S15						
			versions < V4.8 HF6),							
			SINAMICS S150 V5.1 (All							
					versions), SINAMICS S150 V5.1 SP1 (All versions < V5.1					
			V5.1 S	SPI (All	versions	s < V5.1			<u> </u>	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; Dos-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			SP1 HF4), SINAMICS S210 V5.1 (All versions), SINAMICS S210 V5.1 SP1 (All versions), SITOP Manager (All versions), SITOP PSU8600 (All versions), SITOP UPS1600 (All versions), TIM 1531 IRC (All versions). The webserver of the affected devices contains a vulnerability that may lead to a denial-of-service condition. An attacker may cause a denial-of-service situation which leads to a restart of the webserver of the affected device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was		
			known. CVE ID : CVE-2019-6568		
Improper Input Validation	17-04-2019	7.8	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP	N/A	O-SIE-SIMA- 010519/453

0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

CV Scoring Scale

Vulnerability Type(s)	Publish Date	cvss	Descri	ption & CVE	ID	Pa	tch	NCII	PC ID		
			PC2 (All ve	rsions), SII	MATIC						
			IPC DiagMo	onitor (All							
			versions), S	SIMATIC N	ET PC						
			Software (A	All versions	s),						
			SIMATIC R								
			versions), S	•	F600R						
			(All version								
			1500 CPU 1	-							
			versions >:		1ATIC						
			S7-1500 Sc								
			(All version	ns >= V2.5)							
			SIMATIC W	_							
			versions <	•							
			SIMATIC W		<i>J.</i>						
			Advanced (
			SIMATIC W	-							
			Comfort (All versions),								
			SIMATIC W								
			HSP Comfo								
				inCC Runt							
			Mobile (All								
			NMS (All v	_							
			Server (All	-	NEMA						
			SINUMERI		ONTTON						
					erver						
			(All version	-	CA11						
			TeleContro		-						
			versions). S	-							
			network pa								
			affected de	-							
			4840/tcp c								
			unauthenti								
			attacker to								
			Service cor	idition of tl	ne OPC						
			communic	ation or cra							
			device. The	esecurity							
			vulnerabili	ty could be							
			exploited b	-							
			network ac								
			affected sy	stems. Suc	cessful						
CV Scoring Sca	le 0.4	1.2		4.5	ГС	6.7	7.0	0.0	0.4		
(CVSS)	0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-1		

Vulnerability Type(s)	Publish Date	cvss	Description	& CVE ID	Pa	tch	NCIII	PC ID
			exploitation requirements system privilege user interaction could use the vulto compromise at the OPC commutation of advisory publication no presploitation of the vulnerability was a complete.	es and no . An attacker alnerability availability of nication. At sory bublic his security as known.				
tim_1531_irc_	firmware							
Improper Input Validation	pper 17-04-2019 5 ation		A vulnerability identified in CPT versions), CP16 versions), SIAM (All versions), SCP343-1 Advance versions), SIMA (All versions), SIMA (All versions), SIMA OPC UA (All versions < Volume of Controller CPU (All versions), SCOMFORT Outdoor 15" (All versions), SCOMFORT Outdoor 15" (All versions), SCOMFORT Outdoor 15" (All versions), SCOMFORT OUTDOOR (All versions)	1604 (All 16 (All TIC RF185C IMATIC ced (All TIC CP443-1 IMATIC ced (All TIC CP443-1 sions), 0 SP Open 1515SP PC 72.1.6), 0 SP Open 1515SP PC2 IMATIC HMI or Panels 7" & s), SIMATIC cnels 4" - 22" IMATIC HMI els KTP400F, 0F, KTP900 All versions), agMonitor	N/A		O-SIE- 01051	_
CV Scoring Scale	e 0-1	1-2	2-3 3-4		6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	D	escriptio	n & CVE	ID	Pa	tch	NCIII	PC ID
			RF181	-EIP (Al	l versio	ns),				
			SIMAT	IC RF18	2C (All					
			versioi	ns), SIM	ATIC RI	F186C				
			(All versions), SIMATIC							
			RF188	C (All ve	ersions)	,				
			SIMAT	IC RF60	OR (All					
			versio	ns), SIM	ATIC S7	-1500				
			CPU fa	mily (Al	l versio	ns),				
			SIMAT	IC S7-15	500 Sof	ware				
	Controller (All versions),									
		family								
			(All ve	rsions <	V3.X.1	6),				
			SIMAT	IC S7-40	00 PN (i	ncl. F)				
			V6 and	below	(All ver	sions),				
			SIMAT	IC S7-40	00 PN/I	OP V7				
			(incl. F) (All ve	rsions)	,				
			SIMAT	IC S7-PI	LCSIM					
			Advan	ced (All	version	s),				
			SIMAT	IC Teles	ervice					
			Adapte	er IE Adv	anced	(All				
				ns), SIM						
			Telese	rvice Ad	apter Il	E Basic				
				rsions),	_					
			_	rvice Ad						
				rd (All v	_					
				IC WinA		-				
			(All ve	rsions),	SIMATI	C				
			`	Runtim						
				rsions),						
			`	EIP (All v						
			•	ODE pro		-				
				ns), SINA						
				All versi		.100				
			`	ICS G13	-	(A))				
				ns), SIN <i>I</i>						
			V4.7 SP1 (All versions), SINAMICS G130 V4.8 (All							
			,							
			versions < V4.8 HF6), SINAMICS G130 V5.1 (All							
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
(CVSS) Vulnerability Ty										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	tch	NCIII	PC ID
			versions), SINAMICS G130				
			V5.1 SP1 (All versions < V	5.1			
			SP1 HF4), SINAMICS G150				
			V4.6 (All versions),				
			SINAMICS G150 V4.7 (All				
			versions), SINAMICS G150				
			V4.7 SP1 (All versions),				
			SINAMICS G150 V4.8 (All				
			versions < V4.8 HF6),				
			V5.1 SP1 (All versions < V	5.1			
			SP1 HF4), SINAMICS S120				
			V4.6 (All versions),				
			SINAMICS S120 V4.7 (All				
			versions), SINAMICS \$120				
			V4.7 SP1 (All versions),				
			SINAMICS S120 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S120 V5.1 (All				
			versions), SINAMICS \$120				
			V5.1 SP1 (All versions < V				
			SP1 HF4), SINAMICS S150				
			V4.6 (All versions),				
			SINAMICS S150 V4.7 (All				
			versions), SINAMICS S150				
			V4.7 SP1 (All versions),				
			SINAMICS S150 V4.8 (All				
			versions < V4.8 HF6),				
			SINAMICS S150 V5.1 (All				
			versions), SINAMICS S150				
			V5.1 SP1 (All versions < V				
			SP1 HF4), SINAMICS S210				
			V5.1 (All versions),				
			SINAMICS S210 V5.1 SP1				
			(All versions), SITOP				
			Manager (All versions),				
			• •				
			SITOP PSU8600 (All versions), SITOP UPS1600				
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-1		7-8	8-9	9-1
(CVSS)	0-1	1 2	2-3 3-4 4-3 3-1	0-7	7-0	0-3	5-10

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCIII	PC ID
			(All von websed devices vulne to a decondition of the after security with a se	evice. At ory publ e exploit ity vulne	The the affectins a service attacker of-service. The ads webserve attacker of attacker access the a	r lead r lead r may ice to a rer of ne could acker o the cessful no no ttacker bility bility of e of no this was				
simatic_cp443	3-1_opc_ua_fi	rmwar	•	1 .1.			T		T	
Improper Input Validation	17-04-2019	7.8	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP PC2 (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC NET PC Software (All versions), SIMATIC RF188C (All versions), SIMATIC RF600R			N/A		0-SIE- 01051	SIMA- 9/455	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross	Site Rea	uest Fore	rory: Dir 1	ray Diro	ctory Trav	orcal: ±In	fo- Gain Ir	formatio	n· DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pat	ch	NCIII	PC ID
			(All versions), SIMATIC S7-				
			1500 CPU family (All				
			versions >= V2.5), SIMATIC				
			S7-1500 Software Controlle	er			
			(All versions >= V2.5),				
			SIMATIC WinCC OA (All				
			versions < V3.15-P018),				
			SIMATIC WinCC Runtime				
			Advanced (All versions),				
			SIMATIC WinCC Runtime				
			Comfort (All versions),				
			SIMATIC WinCC Runtime				
			HSP Comfort (All versions)				
			SIMATIC WinCC Runtime				
			Mobile (All versions), SINE	<u></u>			
			NMS (All versions), SINEMA				
			Server (All versions),				
			SINUMERIK OPC UA Server				
			(All versions < V2.1),				
			TeleControl Server Basic (A	.11			
			versions). Specially crafted				
			network packets sent to				
			affected devices on port				
			4840/tcp could allow an				
			unauthenticated remote				
			attacker to cause a Denial-o	.f			
			Service condition of the OP				
			communication or crash th				
				2			
			device. The security				
			vulnerability could be	.,			
			exploited by an attacker wi	tn			
			network access to the				
			affected systems. Successfu	l			
			exploitation requires no				
			system privileges and no				
			user interaction. An attacke	er			
			could use the vulnerability				
			to compromise availability				
			the OPC communication. At				
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty	0 1		2 3 3 3 3 6	- 0 /	, 0	3 3	7 10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Pa	tch	NCIII	PCID
			the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6575				
simatic_et_20	0_open_contr	oller_c	pu_1515sp_pc2_firmware				
Improper Input Validation	17-04-2019	7.8	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP PC2 (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC NET PC Software (All versions), SIMATIC RF188C (All versions), SIMATIC RF600R (All versions), SIMATIC S7-1500 CPU family (All versions >= V2.5), SIMATIC S7-1500 Software Controller (All versions <= V2.5), SIMATIC WinCC OA (All versions < V3.15-P018), SIMATIC WinCC Runtime Advanced (All versions), SIMATIC WinCC Runtime Comfort (All versions), SIMATIC WinCC Runtime HSP Comfort (All versions), SIMATIC WinCC Runtime HSP Comfort (All versions), SIMATIC WinCC Runtime Mobile (All versions), SINECNMS (All versions), SINECNMS (All versions), SINEMA Server (All versions). Specially crafted	N/A		O-SIE- 01051	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
		_	uest Forgery; Dir. Trav Directory Travoss Site Scripting; Sql- SQL Injection; N 395			nformation	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	1	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			affect 4840, unaut attack Service comm device vulne explo netwo affect explo system user i could to cor the Of the tin public explo vulne	ed device the countries to cause the condition of additation or rability and cation references the commission of additation or rability and cation and cation or rability and cation and cation or rability and cation and cati	could be an attack ss to the ms. Succe equires eges and on. An a vulnera se availa nunicati visory	ort an ote inial-of- ne OPC ash the er with cessful no no ttacker bility bility of on. At curity wn.				
simatic_ipc_di	iagmonitor_fi	rmwar	·e							
Improper Input Validation	17-04-2019	7.8	identi CP44: versic Open PC2 (A IPC D: versic Softw SIMA' versic (All versic (All versic	A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200 Open Controller CPU 1515SP PC2 (All versions), SIMATIC IPC DiagMonitor (All versions), SIMATIC NET PC Software (All versions), SIMATIC RF188C (All versions), SIMATIC RF600R (All versions), SIMATIC S7-1500 CPU family (All versions >= V2.5), SIMATIC		N/A			-SIMA- .9/457	
CV Scoring Scale			2-3	3-4	4-5	5-6	6-7	7-8	8-9	

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID				Pat	tch	NCIII	PC ID
			S7-150	00 Softw	are Cor	ntroller				
			(All ve	rsions >	= V2.5)	,				
			SIMAT	IC Win(CC OA (A	All				
			version	ns < V3.	15-P01	3),				
			SIMAT	IC Win(CC Runti	ime				
			Advan	ced (All	version					
			SIMAT	IC Win(CC Runti					
			Comfo	rt (All v	ersions),				
				•	CC Runti					
			HSP Co	mfort (All vers	ions).				
				-	CC Runt	-				
					rsions),					
				•	ons), SI					
			`	(All ver		TTI-III				
				•	PC UA S	erver				
				rsions <		CIVCI				
			-		_	sic (All				
				TeleControl Server Basic (All						
			versions). Specially crafted network packets sent to							
				_	es on po					
					•					
			-	_	d allow ed remo					
						nial-of-				
					ion of th					
					n or cra	ish the				
				The se	•					
				•	ould be					
			-	•		er with				
					s to the					
			affecte	d syster	ns. Succ	essful				
			exploit	ation re	equires	no				
			system	privile	ges and	no				
			user in	teractio	n. An at	ttacker				
			could ι	ise the v	vulnera	bility				
			to com	promis	e availa					
			the OPC communication. At							
			the time of advisory							
				ation no						
			-		this se	curity				
CV Scoring Sca	le	4.0		2.4		F 6	6.7	- .	0.6	
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID					itch	NCII	PC ID
			vulne	rability	was kno	wn.				
			CVE I	D : CVE-	2019-6	575				
simatic_net_p	c_software_fi	rmwar	e							
Improper Input Validation	17-04-2019	7.8	identi CP44: versic Open PC2 (A IPC Diversic Softw SIMA' versic ST-15 (All versic SIMA' Advan SIMA' Advan SIMA' NMS (SIMA' Mobil NMS (SIMA' Mobil NMS (All versic SINUN (All v	nerability fied in S 3-1 OPC ons), SIM Control All versity iagMonity ons), SIM ersions), SIM ersions; CPU fam ons < V3 CPU fam ons > E ons), SIM ersions; CPU fam ons > E ons >	IMATIC UA (All IATIC E' ler CPU ons), SII tor (All IATIC NI IATIC NI IATIC NI IATIC NI IATIC NI IATIC RI IATIC	F 200 1515SP MATIC ET PC s), F600R IC S7- MATIC ntroller , All 8), ime is), ime sions), ime SINEC- NEMA Gerver asic (All rafted to ort	N/A			-SIMA- 19/458
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	pe(s): CSRF- Cross	Site Req	uest For	gery; Dir. 1	rav Dire	ctory Trav	ersal; +In	fo- Gain I	nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
			unauthenticated remote attacker to cause a Denial-of-Service condition of the OPC communication or crash the device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the OPC communication. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID: CVE-2019-6575							
6ed1052-1cc	01-0ba8_firm	ware								
Uncontrolled Resource Consumption	17-04-2019	5	ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO - Programmable Logic Controllers, multiple versions. Researchers have found some controllers are susceptible to a denial-of- service attack due to a flood of network packets. CVE ID: CVE-2019-10953				N/A			-6ED1- 19/459
6es7211-1ae4	40-0xb0_firm	ware								
Uncontrolled Resource Consumption	17-04-2019	5	ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO - Programmable Logic Controllers, multiple versions. Researchers have				N/A			-6ES7- 19/460
CV Scoring Scal (CVSS)	e 0-1 pe(s): CSRF- Cross	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
vunterability Ty	Denial of Service	_				_			normatio	iii, D03-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			found some controllers are susceptible to a denial-of-service attack due to a flood of network packets.		
			CVE ID : CVE-2019-10953		
6es7314-6eh	04-0ab0_firm	ware			
Uncontrolled Resource Consumption	17-04-2019	5	ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO - Programmable Logic Controllers, multiple versions. Researchers have found some controllers are susceptible to a denial-of- service attack due to a flood of network packets.	N/A	O-SIE-6ES7- 010519/461
			CVE ID : CVE-2019-10953		
Trendnet					·
tv-ip110wn_f	irmware				
Improper Restriction of Operations	22-04-2019	7.5	system.cgi on TRENDnet TV-IP110WN cameras has a buffer overflow caused by an inadequate source-length check before a strcpy operation in the respondAsp function. Attackers can exploit the vulnerability by	N/A	O-TRE-TV-I- 010519/462
within the Bounds of a Memory Buffer			using the languse parameter with a long string. This affects 1.2.2 build 28, 64, 65, and 68. CVE ID: CVE-2019-11417		
Bounds of a Memory	irmware		using the languse parameter with a long string. This affects 1.2.2 build 28, 64, 65, and 68.		
Bounds of a Memory Buffer	firmware 22-04-2019	7.5	using the languse parameter with a long string. This affects 1.2.2 build 28, 64, 65, and 68.	N/A	O-TRE-TEW- - 010519/463
Bounds of a Memory Buffer tew-632brp_1 Improper Restriction	22-04-2019	7.5	using the languse parameter with a long string. This affects 1.2.2 build 28, 64, 65, and 68. CVE ID: CVE-2019-11417 apply.cgi on the TRENDnet TEW-632BRP 1.010B32	N/A 6-7 7-8	-

Vulnerability Type(s)	Publish Date	cvss	ı	Description	on & CVE	ID	Pa	tch	NCII	PC ID
Operations within the Bounds of a				ng string ACTION ace.						
Memory Buffer			CVE I	D : CVE-	2019-1	1418				
Wago										
bacnet/ip_firm	mware									
Uncontrolled Resource Consumption	17-04-2019	5	Schne WAG(Logic versic found susce service	Phoenix ider Ele O - Progr Control ons. Rese some co ptible to e attack work pa	ctric, Sie rammab lers, mul earchers ontroller a denia due to a	emens, le ltiple have rs are l-of-	N/A		0-WA BACN 01051	
			CVE I	D : CVE-	2019-1	0953				
ethernet_firm	iware									
Uncontrolled Resource Consumption	17-04-2019	5	Schne WAGO Logic versic found susce servic of net	ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO - Programmable Logic Controllers, multiple versions. Researchers have found some controllers are susceptible to a denial-of- service attack due to a flood of network packets. CVE ID: CVE-2019-10953					O-WA ETHE- 01051	
knx_ip_firmw	are									
Uncontrolled Resource Consumption	17-04-2019	5	ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO - Programmable Logic Controllers, multiple versions. Researchers have found some controllers are susceptible to a denial-of-			N/A		0-WA KNX 01051		
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service								nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID					tch	NCI	IPC ID		
				e attack work pa		flood						
			CVE I	D : CVE-	2019-1	0953						
pfc100_firmw	are											
Uncontrolled Resource Consumption	17-04-2019	7-04-2019 5		susceptible to a denial-of- service attack due to a flood of network packets.				Schneider Electric, Siemens, WAGO - Programmable Logic Controllers, multiple versions. Researchers have found some controllers are susceptible to a denial-of- service attack due to a flood			O-WA PFC1- 0105	
xinruidz												
sundray_wan	_controller_fi	rmwar	e									
Use of Hard- coded Credentials	18-04-2019	10	WAC on the Sangfor Sundray WLAN Controller version 3.7.4.2 and earlier has a backdoor account allowing a remote attacker to login to the system via SSH (on TCP				N/A		O-XIN SUND 0105			
Improper Neutralizatio n of Special Elements used in a Command ('Command	18-04-2019	10	WAC on the Sangfor Sundray WLAN Controller version 3.7.4.2 and earlier has a Remote Code Execution issue allowing remote attackers to achieve full access to the system, because shell				N/A		O-XIN SUND 0105			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
	pe(s): CSRF- Cross	Site Req	uest For	gery; Dir. 1	rav Dire	ctory Trav	ersal; +In	fo- Gain I	nformation	on; DoS-		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Injection')			metacharacters in the nginx_webconsole.php Cookie header can be used to read an etc/config/wac/wns_cfg_ad min_detail.xml file containing the admin password. (The password for root is the WebUI admin password concatenated with a static string.) CVE ID: CVE-2019-9161		
Intel			Hardware		
-					
Information Exposure	17-04-2019	2.1	Memory access in virtual memory mapping for some microprocessors may allow an authenticated user to potentially enable information disclosure via local access. CVE ID: CVE-2019-0162	https://www .intel.com/co ntent/www/ us/en/securi ty- center/advis ory/intel-sa- 00238.html	H-INT 010519/470

CV Scoring Scale	0.1	1.2	2.2	2.4	4 5	5-6	6.7	7.0	0 N	0.10
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-0	6-7	7-8	8-9	9-10