



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	Patch	NCIIPC ID
Application					
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=admin&a=add URI. CVE ID : CVE-2019-11374	N/A	A-74C-74CM-010519/1
Apache					
pony_mail					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2019	4.3	A vulnerability was discovered wherein a specially crafted URL could enable reflected XSS via JavaScript in the pony mail interface. CVE ID : CVE-2019-0218	N/A	A-APA-PONY-010519/2
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-010519/3
aquaverde					
aquarius_cms					

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
Information Exposure Through Log Files	24-04-2019	5	aquaverde Aquarius CMS through 4.3.5 allows Information Exposure through Log Files because of an error in the Log-File writer component. CVE ID : CVE-2019-9724	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	An issue was discovered in Artifex MuJS 1.0.5. The Number#toFixed() and numtostr implementations in jsnumber.c have a stack-based buffer overflow. CVE ID : CVE-2019-11411	N/A	A-ART-MUJS-010519/5
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. CVE ID : CVE-2019-11412	N/A	A-ART-MUJS-010519/6
Uncontrolled Resource Consumption	22-04-2019	5	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-010519/7

atftp_project

atftp

Improper Restriction	20-04-2019	7.5	An issue was discovered in atftpd in atftp 0.7.1. A	N/A	A-ATF-ATFT-
----------------------	------------	-----	---	-----	-------------

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					
of Operations within the Bounds of a Memory Buffer			remote attacker may send a crafted packet triggering a stack-based buffer overflow due to an insecurely implemented strncpy call. The vulnerability is triggered by sending an error packet of 3 bytes or fewer. There are multiple instances of this vulnerable strncpy pattern within the code base, specifically within tftpd_file.c, tftp_file.c, tftpd_mtftp.c, and tftp_mtftp.c. CVE ID : CVE-2019-11365		010519/8					
NULL Pointer Dereference	20-04-2019	4.3	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 service attack due to a NULL pointer dereference. If thread_data is NULL when assigned to current, and modified by another thread before a certain tftpd_list.c check, there is a crash when dereferencing current->next. CVE ID : CVE-2019-11366	N/A	A-ATF-ATFT-010519/9					
Atlassian										
confluence										
Improper Limitation of	18-04-2019	9	Confluence Server and Data Center had a path traversal	N/A	A-ATL-CONF-					
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
a Pathname to a Restricted Directory ('Path Traversal')			<p>vulnerability in the downloadallattachments resource. A remote attacker who has permission to add attachments to pages and / or blogs or to create a new space or a personal space or who has 'Admin' permissions for a space can exploit this path traversal vulnerability to write files to arbitrary locations which can lead to remote code execution on systems that run a vulnerable version of Confluence Server or Data Center. All versions of Confluence Server from 2.0.0 before 6.6.13 (the fixed version for 6.6.x), from 6.7.0 before 6.12.4 (the fixed version for 6.12.x), from 6.13.0 before 6.13.4 (the fixed version for 6.13.x), from 6.14.0 before 6.14.3 (the fixed version for 6.14.x), and from 6.15.0 before 6.15.2 are affected by this vulnerability.</p> <p>CVE ID : CVE-2019-3398</p>		010519/10

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-010519/11
---	------------	-----	---	-----	----------------------

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
			<p>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.</p> <p>CVE ID : CVE-2019-11446</p>		
Blackberry					
unified_endpoint_management					
Improper Restriction of XML External Entity Reference ('XXE')	18-04-2019	5	<p>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.</p> <p>CVE ID : CVE-2019-8999</p>	N/A	A-BLA-UNIF-010519/12
brassica					
soy_cms					
Improper Control of Generation of Code ('Code Injection')	20-04-2019	6.5	<p>** DISPUTED ** SOY CMS 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."</p> <p>CVE ID : CVE-2019-11376</p>	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
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
burrow-wheeler_aligner_project					
burrow-wheeler_aligner					
Improper Restriction of Operations within the Bounds of a Memory Buffer	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): 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
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_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): 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					
			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 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_computing_system										
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-UNIF-010519/19					
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					
			be allowed for a specific subset of local management CLI commands. The vulnerability is due to lack of proper input validation of user input for local management CLI commands. An attacker could exploit this vulnerability by authenticating to the device and issuing a crafted form of a limited subset of local management CLI commands. An exploit could allow the attacker to overwrite an arbitrary files on disk or inject CLI command parameters that should have been disabled. This vulnerability is fixed in software version 4.0(2a) and later. CVE ID : CVE-2019-1725							
registered_envelope_service										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	3.5	A vulnerability in the web-based interface of the Cisco Registered Envelope Service could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against another user of the service. The vulnerability is due to insufficient validation of user-supplied input by the web-based interface of the affected software. An attacker could exploit this	N/A	A-CIS-REGI-010519/20					
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
			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 Neutralization 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 browser-based information. This vulnerability has been fixed in the current version of Cisco Umbrella. Cisco	N/A	A-CIS-UMBR-010519/21
--	------------	-----	--	-----	----------------------

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
			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. CVE ID : CVE-2019-1796	N/A	A-CIS-WIRE-010519/22
Cross-Site Request Forgery (CSRF)	17-04-2019	6.8	A vulnerability in the web-based management interface of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary	N/A	A-CIS-WIRE-010519/23

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
			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

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					
			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. CVE ID : CVE-2019-1799							
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. CVE ID : CVE-2019-1800	N/A	A-CIS-WIRE-010519/25					
wireless_lan_controller_software										
Improper Access Control	17-04-2019	3.3	A vulnerability in certain access control mechanisms for the Secure Shell (SSH)	N/A	A-CIS-WIRE-010519/26					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
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
			<p>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 input- and 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).</p> <p>CVE ID : CVE-2019-1805</p>		
Improper Input Validation	17-04-2019	6.8	<p>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</p>	N/A	A-CIS-WIRE-010519/27

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
			<p>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.</p> <p>CVE ID : CVE-2019-1830</p>		

email_security_appliance

Improper Input Validation	17-04-2019	5	<p>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.</p>	N/A	A-CIS-EMAI-010519/28
---------------------------	------------	---	--	-----	----------------------

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					
			CVE ID : CVE-2019-1831							
unified_communications_manager										
Improper Input Validation	17-04-2019	7.8	A vulnerability in the User Data Services (UDS) API of Cisco Unified Communications Manager (Unified CM) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the management GUI. The vulnerability is due to improper validation of input parameters in the UDS API requests. An attacker could exploit this vulnerability by sending a crafted request to the UDS API of an affected device. A successful exploit could allow the attacker to make the A Cisco DB service quit unexpectedly, preventing admin access to the Unified CM management GUI. Manual intervention may be required to restore normal operation. Software versions 10.5, 11.5, 12.0, 12.5 are affected. CVE ID : CVE-2019-1837	N/A	A-CIS-UNIF-010519/29					
prime_network_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-PRIM-010519/30					
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
			<p>the server and cause a denial of service (DoS) condition on the affected system. The vulnerability is due to incomplete user-supplied input validation when a custom extension attempts to change a DHCPv6 packet received by the application. An attacker could exploit this vulnerability by sending malformed DHCPv6 packets to the application. An exploit could allow the attacker to trigger a restart of the service which, if exploited repeatedly, might lead to a DoS condition. This vulnerability can only be exploited if the administrator of the server has previously installed custom extensions that attempt to modify the packet details before the packet has been processed. Note: Although the CVSS score matches a High SIR, this has been lowered to Medium because this condition will only affect an application that has customer-developed extensions that will attempt to modify packet parameters before the packet has been completely sanitized. If packet modification in a custom extension happens after the packet has been</p>		

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
			sanitized, the application will not be affected by this vulnerability. Software versions prior to 8.3(7) and 9.1(2) are affected. CVE ID : CVE-2019-1840		

firepower_management_center

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	3.5	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected system. The vulnerability is due to insufficient validation of user-supplied input in the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user to access a report containing malicious content. 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. Versions 6.2.3, 6.3.0, and 6.4.0 are affected. CVE ID : CVE-2019-1802	N/A	A-CIS-FIRE-010519/31
--	------------	-----	---	-----	----------------------

identity_services_engine

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
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 Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	3.5	A vulnerability in the web-based guest portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based 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

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					
			a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive browser-based information. Cisco ISE software version 2.1 is affected. CVE ID : CVE-2019-1719							
meeting_server										
Uncontrolled Search Path Element	17-04-2019	3.6	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-MEET-010519/34					
telepresence_video_communication_server										
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-TELE-010519/35					
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
			<p>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.</p> <p>CVE ID : CVE-2019-1720</p>		
N/A	17-04-2019	6.8	<p>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</p>	N/A	A-CIS-TELE-010519/36

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
			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. CVE ID : CVE-2019-1721		
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

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
			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		

Cloudbees

jenkins_operations_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	N/A	A-CLO-JENK-010519/38
-----	------------	---	--	-----	----------------------

cloudfoundry

capi-release

Improper Authentication	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.cloudfoundry.org/blog/cve-2019-3798	A-CLO-CAPI-010519/39
-------------------------	------------	---	---	---	----------------------

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					
			and knowledge of the email of a victim in the foundation may escalate their privileges to that of the victim by creating a client with a name equal to the guid of their victim. CVE ID : CVE-2019-3798							
Clusterlabs										
pacemaker										
Use After Free	18-04-2019	5	A use-after-free flaw was 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	N/A	A-CLU-PACE-010519/40					
Cmsmadesimple										
cms_made_simple										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-04-2019	3.5	The File Manager in CMS Made Simple through 2.2.10 has Reflected XSS via the "New name" field in a Rename action. CVE ID : CVE-2019-11513	N/A	A-CMS-CMS_-010519/41					
Contao										
contao_cms										
Weak Password Recovery Mechanism for Forgotten Password	17-04-2019	5	Contao before 3.5.39 and 4.x before 4.7.3 has a Weak Password Recovery Mechanism for a Forgotten Password.	https://contao.org/en/news/security-vulnerability-cve-2019-10641.html	A-CON-CONT-010519/42					
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
			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://contao.org/en/news/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://contao.org/en/news/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 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
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 Heap-based 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 Heap-based 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 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					
			when the user opens a malformed PDF file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. CVE ID : CVE-2019-9139							
Dell										
emc_isilon_sd_management_server										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	4.3	IsilonSD Management Server 1.1.0 contains a cross-site scripting vulnerability while uploading an OVA file. A remote attacker can trick an admin user to potentially exploit this vulnerability to execute malicious HTML or JavaScript code in the context of the admin user. CVE ID : CVE-2019-3708	N/A	A-DEL-EMC_-010519/50					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-04-2019	4.3	IsilonSD Management Server 1.1.0 contains a cross-site scripting vulnerability while registering vCenter servers. A remote attacker can trick an admin user to potentially exploit this vulnerability to execute malicious HTML or JavaScript code in the context of the admin user. CVE ID : CVE-2019-3709	N/A	A-DEL-EMC_-010519/51					
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-DEL-SUPP-010519/52					
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
(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

cncsoft_screeneditor

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
---	------------	-----	--	-----	----------------------

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
			copying data from project files onto the stack. CVE ID : CVE-2019-10947		
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	N/A	A-DEL-CNCS-010519/55
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 specially crafted project files, allowing an attacker to remotely execute arbitrary code. There is a lack of user input validation before copying data from project files onto the heap. CVE ID : CVE-2019-10951	N/A	A-DEL-CNCS-010519/56

Drupal

drupal

Improper Neutralization 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-010519/57
---	------------	-----	--	-----	----------------------

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
Page Generation ('Cross-site Scripting')			jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype. CVE ID : CVE-2019-11358		

EA

origin

Improper Control of Generation of Code ('Code Injection')	19-04-2019	6.8	The client in Electronic Arts (EA) Origin 10.5.36 on Windows allows template injection in the title parameter of the Origin2 URI handler. This can be used to escape the underlying AngularJS sandbox and achieve remote code execution via an origin2://game/launch URL for QApplication QDesktopServices communication. CVE ID : CVE-2019-11354	N/A	A-EA-ORIG-010519/58
---	------------	-----	---	-----	---------------------

Eclipse

jetty

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2019	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	https://bugs.eclipse.org/bugs/show_bug.cgi?id=546121	A-ECL-JETT-010519/59
--	------------	-----	---	---	----------------------

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
			configured for showing a Listing of directory contents. CVE ID : CVE-2019-10241		
Fedoraproject					
389_directory_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-04-2019	5	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 un-encrypted 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	https://pagure.io/389-ds-base/pull-request/50331	A-FED-389_-010519/60
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-010519/61

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
			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 Authentication	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. CVE ID : CVE-2019-11234	N/A	A-FRE-FREE-010519/63
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 (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
gbraad					
gauth					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-04-2019	4.3	GAAuth 0.9.9 beta has stored XSS that shows a popup repeatedly and discloses cookies. CVE ID : CVE-2019-11084	https://github.com/gbraad/gauth/issues/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?download= 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://gitlab.com/gitlab-org/gitlab-ce/issues/42726	A-GIT-GITL-010519/68

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
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://gitlab.com/gitlab-org/gitlab-ce/issues/51971	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://gitlab.com/gitlab-org/gitlab-ce/issues/54635	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). CVE ID : CVE-2019-9172	https://gitlab.com/gitlab-org/gitlab-ce/issues/54795	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://gitlab.com/gitlab-org/gitlab-ce/issues/55468	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://gitlab.com/gitlab-org/gitlab-ce/issues/52524	A-GIT-GITL-010519/73

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
			(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. CVE ID : CVE-2019-9176	https://gitlab.com/gitlab-org/gitlab-ce/issues/55664	A-GIT-GITL-010519/74
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). CVE ID : CVE-2019-9178	https://gitlab.com/gitlab-org/gitlab-ce/issues/54803	A-GIT-GITL-010519/75
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). CVE ID : CVE-2019-9179	https://gitlab.com/gitlab-org/gitlab-ce/issues/54783	A-GIT-GITL-010519/76
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://gitlab	A-GIT-GITL-

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
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/54159	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://gitlab.com/gitlab-org/gitlab-ce/issues/55653	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://gitlab.com/gitlab-org/gitlab-ce/issues/56348	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://gitlab.com/gitlab-org/gitlab-ce/issues/50334	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://gitlab.com/gitlab-org/gitlab-ce/issues/54789	A-GIT-GITL-010519/82

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
			has Incorrect Access Control (issue 4 of 5). CVE ID : CVE-2019-9224		
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 (issue 5 of 5). CVE ID : CVE-2019-9225	https://gitlab.com/gitlab-org/gitlab-ce/issues/54680	A-GIT-GITL-010519/83
Improper Access Control	17-04-2019	7.5	An issue was discovered in GitLab Community and Enterprise Edition 10.x (starting from 10.8) and 11.x before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control, a different vulnerability than CVE-2019-9732. CVE ID : CVE-2019-9756	https://gitlab.com/gitlab-org/gitlab-ce/issues/54243	A-GIT-GITL-010519/84
N/A	17-04-2019	6.4	An issue was discovered in GitLab Community and Enterprise Edition 10.x and 11.x 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-2019-9890	N/A	A-GIT-GITL-010519/85

Gnome

evince

Access of Uninitialized Pointer	22-04-2019	4.3	The tiff_document_render() and tiff_document_get_thumbnail	N/A	A-GNO-EVIN-010519/86
---------------------------------	------------	-----	--	-----	----------------------

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
			<p>() functions in the TIFF document backend in GNOME Evince through 3.32.0 did not handle errors from TIFFReadRGBAImageOriented(), leading to uninitialized memory use when processing certain TIFF image files.</p> <p>CVE ID : CVE-2019-11459</p>		
gnome-desktop					
Improper Input Validation	22-04-2019	6.8	<p>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.</p> <p>CVE ID : CVE-2019-11460</p>	N/A	A-GNO-GNOM-010519/87
Google					
tensorflow					
NULL	24-04-2019	4.3	NULL pointer dereference in	N/A	A-GOO-

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
Pointer Dereference			Google TensorFlow before 1.12.2 could cause a denial of service via an invalid GIF file. CVE ID : CVE-2019-9635		TENS-010519/88
Gradle					
enterprise					
N/A	22-04-2019	5	In Gradle Enterprise before 2018.5.3, Build Cache Nodes did not store the credentials at rest in an encrypted format. CVE ID : CVE-2019-11402	N/A	A-GRA-ENTE-010519/89
N/A	22-04-2019	5	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. CVE ID : CVE-2019-11403	N/A	A-GRA-ENTE-010519/90
Graphicsmagick					
graphicsmagick					
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-010519/91

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
			CVE ID : CVE-2019-11505		
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-04-2019	6.8	In GraphicsMagick from version 1.3.30 to 1.4 snapshot-20190403 Q8, there is a heap-based buffer overflow in the function WriteMATLABImage of coders/mat.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 ExportRedQuantumType in magick/export.c. CVE ID : CVE-2019-11506	N/A	A-GRA-GRAP-010519/92
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-010519/93
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 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					
			CVE ID : CVE-2019-11474							
gstreamer_project										
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	https://gstreamer.freedesktop.org/security/sa-2019-0001.html	A-GST-GSTR-010519/95					
IBM										
sterling_b2b_integrator										
Improper Neutralization 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: 157107. CVE ID : CVE-2019-4073	https://www.ibm.com/support/docview.wss?uid=ibm10880591	A-IBM-STER-010519/96					
Improper Neutralization 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	https://www.ibm.com/support/docview.wss?uid=ibm10880591	A-IBM-STER-010519/97					
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
			leading to credentials disclosure within a trusted session. IBM X-Force ID: 157108. CVE ID : CVE-2019-4074		
Improper Neutralization 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. CVE ID : CVE-2019-4075	https://www.ibm.com/support/docview.wss?uid=ibm10880591	A-IBM-STER-010519/98
Improper Neutralization 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	https://www.ibm.com/support/docview.wss?uid=ibm10880591	A-IBM-STER-010519/99
Improper Neutralization of Input During Web	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	https://www.ibm.com/support/docview.wss?uid=ibm10880591	A-IBM-STER-010519/100

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
Page Generation ('Cross-site Scripting')			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: 157111. CVE ID : CVE-2019-4077	m10880591	
Information Exposure	25-04-2019	3.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 could allow an authenticated user to obtain sensitive document information under unusual circumstances. IBM X-Force ID: 158401. CVE ID : CVE-2019-4146	https://www.ibm.com/support/docview.wss?uid=ibm10880595	A-IBM-STER-010519/101
Improper Neutralization 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: 158414. CVE ID : CVE-2019-4148	https://www.ibm.com/support/docview.wss?uid=ibm10880591	A-IBM-STER-010519/102
Information Exposure	25-04-2019	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/support/docview.wss?uid=ibm10880595	A-IBM-STER-010519/103

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					
			process definition of a business process without permission. IBM X-Force ID: 159231. CVE ID : CVE-2019-4222	m10880595						
content_navigator										
Improper Neutralization 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. CVE ID : CVE-2019-4033	https://www.ibm.com/support/docview.wss?uid=ibm10869046	A-IBM-CONT-010519/104					
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 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					
			CVE ID : CVE-2019-4092							
infosphere_information_server										
Improper Neutralization 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	https://www.ibm.com/support/docview.wss?uid=ibm10881165	A-IBM-INFO-010519/106					
infosphere_information_server_on_cloud										
Improper Neutralization 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	https://www.ibm.com/support/docview.wss?uid=ibm10881165	A-IBM-INFO-010519/107					
idreamsoft										
icms										
Improper Neutralization of Input During Web Page	22-04-2019	4.3	An XSS issue was discovered in app/admincp/template/admincp.header.php in idreamsoft iCMS 7.0.14 via	N/A	A-IDR-ICMS-010519/108					
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
Generation ('Cross-site Scripting')			the admincp.php?app=config tab parameter. CVE ID : CVE-2019-11426		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2019	4.3	An XSS issue was discovered in app/search/search.app.php in idreamsoft iCMS 7.0.14 via the public/api.php?app=search q parameter. CVE ID : CVE-2019-11427	N/A	A-IDR-ICMS-010519/109

i-librarian

I, librarian

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-04-2019	4.3	Cross-site scripting (XSS) vulnerability in display.php in I, Librarian 4.10 allows remote attackers to inject arbitrary web script or HTML via the project parameter. CVE ID : CVE-2019-11359	N/A	A-I-L-I, L-010519/110
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2019	4.3	I, Librarian 4.10 has XSS via the export.php export_files parameter. CVE ID : CVE-2019-11428	N/A	A-I-L-I, L - 010519/111
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2019	4.3	I, Librarian 4.10 has XSS via the notes.php notes parameter. CVE ID : CVE-2019-11449	N/A	A-I-L-I, L - 010519/112

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					
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-010519/113					
Divide By Zero	23-04-2019	4.3	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-by-zero error) by crafting an XWD image file in which the header indicates neither LSB first nor MSB first. CVE ID : CVE-2019-11472	N/A	A-IMA-IMAG-010519/114					
Intel										
graphics_performance_analyzer										
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/content/www/us/en/security-center/advis	A-INT-GRAP-010519/115					
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
			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#doTestConnection 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#doTestConnection 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

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					
jira-ext										
N/A	18-04-2019	4	Jenkins jira-ext Plugin 0.8 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	N/A	A-JEN-JIRA-010519/118					
azure_publishersettings_credentials										
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#doValidateUserNamePassword form validation method allows attackers to initiate a connection to an attacker-specified server. CVE ID : CVE-2019-10304	N/A	A-JEN-XEBI-010519/120					
N/A	18-04-2019	4	A missing permission check in Jenkins XebiaLabs XL	N/A	A-JEN-XEBI-					
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
			Deploy Plugin in the Credential#doValidateUserNamePassword form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. CVE ID : CVE-2019-10305		010519/121
ontrack					
N/A	18-04-2019	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					
jQuery					
Improper Neutralization 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 enumerable __proto__ property, it could extend the native Object.prototype. CVE ID : CVE-2019-11358	N/A	A-JQU-JQUE-010519/123
Kubernetes					
kubernetes					

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
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	A-KUB-KUBE-010519/124

Matrix

sydent

Improper Input Validation	19-04-2019	4.3	util/emailutils.py in Matrix Sydent before 1.0.2 mishandles registration restrictions that are based on e-mail domain, if the allowed_local_3pids option is enabled. This occurs because of potentially unwanted behavior in Python, in which an email.utils.parseaddr call on user@bad.example.net@good.example.com returns the user@bad.example.net substring. CVE ID : CVE-2019-11340	N/A	A-MAT-SYDE-010519/125
---------------------------	------------	-----	--	-----	-----------------------

mediaarea

mediainfo

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
Out-of-bounds Read	20-04-2019	4.3	An out-of-bounds read in MediaInfoLib::File__Tags_Helper::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 URL. CVE ID : CVE-2019-11375	N/A	A-MEI-MSVO-010519/128
miniblog.core_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.cs writes a decoded base64	N/A	A-MIN-MINI-010519/129

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
			string to a file without validating the extension. CVE ID : CVE-2019-9845		
mkcms_project					
mkcms					
Improper Authentication	18-04-2019	6.8	MKCMS 5.0 allows remote attackers to take over arbitrary user accounts by posting a username and e-mail address to ucenter/repass.php, which triggers e-mail transmission with the password, as demonstrated by 123456. CVE ID : CVE-2019-11332	N/A	A-MKC-MKCM-010519/130
Modsecurity					
owasp_modsecurity_core_rule_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. CVE ID : CVE-2019-11387	N/A	A-MOD-OWAS-010519/131
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

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
			attackers to cause a denial of service (ReDOS) by entering a specially crafted string with nested repetition operators. CVE ID : CVE-2019-11388		
Incorrect Regular Expression	20-04-2019	5	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with next# at the beginning and nested repetition operators. CVE ID : CVE-2019-11389	N/A	A-MOD-OWAS-010519/133
Incorrect Regular Expression	20-04-2019	5	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with set_error_handler# at the beginning and nested repetition operators. CVE ID : CVE-2019-11390	N/A	A-MOD-OWAS-010519/134
Incorrect Regular Expression	20-04-2019	5	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-933-APPLICATION-ATTACK-	N/A	A-MOD-OWAS-010519/135

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
			PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with \$a# at the beginning and nested repetition operators. CVE ID : CVE-2019-11391		

Mozilla

firefox

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. CVE ID : CVE-2019-9788	N/A	A-MOZ-FIRE-010519/136
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. 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	N/A	A-MOZ-FIRE-010519/137

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
			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. CVE ID : CVE-2019-9790	N/A	A-MOZ-FIRE-010519/138
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. CVE ID : CVE-2019-9788	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

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
			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. CVE ID : CVE-2019-9788	N/A	A-MOZ-THUN-010519/141
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. CVE ID : CVE-2019-9790	N/A	A-MOZ-THUN-010519/142

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
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					

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					
ntp										
N/A	18-04-2019	7.5	Network Time Protocol (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	N/A	A-NTP-NTP-010519/145					
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. CVE ID : CVE-2019-11445	N/A	A-OPE-OPEN-010519/146					
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://support.f5.com/cs/p/article/K58502649	A-ORA-MYSQ-010519/147					
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
			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-2019-2566		
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://support.f5.com/csp/article/K58502649	A-ORA-MYSQ-010519/148

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
			(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). CVE ID : CVE-2019-2581	https://support.oracle.com/cs/article/K58502649	A-ORA-MYSQL-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://support.oracle.com/cs/article/K58502649	A-ORA-MYSQL-010519/150

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
			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://support.f5.com/csp/article/K54470776	A-ORA-MYSQ-010519/151
Improper Access	23-04-2019	4	Vulnerability in the MySQL Server component of Oracle	https://support.f5.com/csp/article/K54470776	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): 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
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/K54470776	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://support.f5.com/p/article/K54470776	A-ORA-MYSQL-010519/153

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
			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://support.f5.com/cs/p/article/K54470776	A-ORA-MYSQL-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://support.f5.com/cs/p/article/K54470776	A-ORA-MYSQL-010519/155

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
			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-2019-2593		
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://support.oracle.com/cs/article/K52514501	A-ORA-MYSQ-010519/156

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
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://support.f5.com/csp/article/K52514501	A-ORA-MYSQL-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://support.f5.com/csp/article/K52514501	A-ORA-MYSQL-010519/158

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
			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://support.f5.com/cs/p/article/K52514501	A-ORA-MYSQL-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://support.f5.com/cs/p/article/K52514501	A-ORA-MYSQL-010519/160

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
			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). CVE ID : CVE-2019-2617		
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://support.f5.com/cs/p/article/K43540241	A-ORA-MYSQL-010519/161

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
			(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://support.f5.com/csp/article/K43540241	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://support.f5.com/csp/article/K43540241	A-ORA-MYSQ-010519/163

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
			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://support.f5.com/cs/p/article/K43540241	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://support.f5.com/cs/p/article/K43540241	A-ORA-MYSQ-010519/165

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
			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-2019-2626		
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://support.f5.com/csp/article/K32798641	A-ORA-MYSQL-010519/166

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
			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://support.f5.com/csp/article/K32798641	A-ORA-MYSQL-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://support.f5.com/csp/article/K32798641	A-ORA-MYSQL-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): 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
			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://support.f5.com/cs/p/article/K32798641	A-ORA-MYSQL-010519/169

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
			CVE ID : CVE-2019-2631		
Improper Input Validation	23-04-2019	5	<p>Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL 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).</p> <p>CVE ID : CVE-2019-2632</p>	https://support.oracle.com/cs/article/K32798641	A-ORA-MYSQL-010519/170
Improper Input Validation	23-04-2019	1.9	<p>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.</p>	https://support.oracle.com/cs/article/K42793451	A-ORA-MYSQL-010519/171

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
			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://support.f5.com/csp/article/K42793451	A-ORA-MYSQ-010519/172
Improper Input	23-04-2019	3.5	Vulnerability in the MySQL Server component of Oracle	https://support.f5.com/csp/article/K42793451	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): 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
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 Protocol 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/K42793451	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://support.f5.com/cs/p/article/K42793451	A-ORA-MYSQL-010519/174

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
			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://support.f5.com/cs/p/article/K42793451	A-ORA-MYSQL-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://support.f5.com/cs/p/article/K28312671	A-ORA-MYSQL-010519/176

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
			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-2019-2683		
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).	https://support.f5.com/csp/article/K28312671	A-ORA-MYSQL-010519/177

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
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
			CVE ID : CVE-2019-2685		
Improper Input Validation	23-04-2019	4	<p>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).</p> <p>CVE ID : CVE-2019-2686</p>	https://support.f5.com/cs/p/article/K28312671	A-ORA-MYSQL-010519/178
Improper Input Validation	23-04-2019	4	<p>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</p>	https://support.f5.com/cs/p/article/K28312671	A-ORA-MYSQL-010519/179

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
			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://support.f5.com/csp/article/K28312671	A-ORA-MYSQL-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://support.f5.com/csp/article/K04246541	A-ORA-MYSQL-010519/181

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
			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://support.f5.com/cs/p/article/K04246541	A-ORA-MYSQL-010519/182

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
			(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://support.f5.com/cs/p/article/K04246541	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://support.f5.com/cs/p/article/K04246541	A-ORA-MYSQ-010519/184

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					
			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-2019-2694							
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-2019-2695	https://support.f5.com/csp/article/K04246541	A-ORA-MYSQL-010519/185					
jdk										
Improper	23-04-2019	5	Vulnerability in the Java SE,	N/A	A-ORA-JDK-					
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
Access Control			<p>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).</p> <p>CVE ID : CVE-2019-2602</p>		010519/186
Improper Access Control	23-04-2019	4.3	<p>Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 7u211,</p>	N/A	A-ORA-JDK-010519/187

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
			<p>8u202, 11.0.2 and 12; Java SE Embedded: 8u201. 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/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).</p> <p>CVE ID : CVE-2019-2684</p>		
Improper Access	23-04-2019	6.8	Vulnerability in the Java SE component of Oracle Java SE	N/A	A-ORA-JDK-010519/188

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
Control			<p>(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).</p> <p>CVE ID : CVE-2019-2697</p>		
Improper Access Control	23-04-2019	6.8	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D).	N/A	A-ORA-JDK-010519/189

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
			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-2019-2698		
Improper Access Control	23-04-2019	6.8	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Windows DLL). The supported version	https://support.f5.com/cs/p/article/K02771314	A-ORA-JDK-010519/190

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					
			that is affected is Java SE: 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. While the vulnerability is in Java SE, attacks may significantly impact additional products. 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 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 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H). CVE ID : CVE-2019-2699							
outside_in_technology										
Improper Access	23-04-2019	7.5	Vulnerability in the Oracle Outside In Technology	N/A	A-ORA-OUTS-					
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
Control			<p>component of Oracle Fusion Middleware (subcomponent: Outside In Filters).</p> <p>Supported versions that are affected are 8.5.3 and 8.5.4.</p> <p>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 update, insert or delete access to some of Oracle Outside In Technology accessible data as well as 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</p>		010519/191

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
			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

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
			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

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
			<p>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).</p> <p>CVE ID : CVE-2019-2610</p>		
Improper Access Control	23-04-2019	6.4	<p>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</p>	N/A	A-ORA-OUTS-010519/194

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
			<p>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).</p> <p>CVE ID : CVE-2019-2611</p>		
Improper Access Control	23-04-2019	6.4	<p>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</p>	N/A	A-ORA-OUTS-010519/195

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
			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). CVE ID : CVE-2019-2612		
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

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
			<p>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).</p> <p>CVE ID : CVE-2019-2613</p>		
Improper Access Control	23-04-2019	6.4	<p>Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are</p>	N/A	A-ORA-OUTS-010519/197

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
			<p>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).</p>		

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
			CVE ID : CVE-2019-2705		
vm_virtualbox					
Improper Access Control	23-04-2019	2.1	<p>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).</p> <p>CVE ID : CVE-2019-2574</p>	N/A	A-ORA-VM_V-010519/198
Improper Input Validation	23-04-2019	4.6	<p>Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are</p>	N/A	A-ORA-VM_V-010519/199

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
			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

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
			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:L/PR:L/UI:N/S:U/C:H/I:H/A:H). CVE ID : CVE-2019-2657		
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-010519/201

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
			CVE ID : CVE-2019-2678		
Improper Input Validation	23-04-2019	3.6	<p>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 ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 7.3 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:H).</p> <p>CVE ID : CVE-2019-2679</p>	N/A	A-ORA-VM_V-010519/202
Improper Input	23-04-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of	N/A	A-ORA-VM_V-

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
Validation			<p>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).</p> <p>CVE ID : CVE-2019-2680</p>		010519/203
Improper Access Control	23-04-2019	4.4	<p>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</p>	N/A	A-ORA-VM_V-010519/204

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
			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		
Improper Access Control	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,	N/A	A-ORA-VM_V-010519/205

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
			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): 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
			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-2019-2721		
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

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
			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

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					
			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							
transportation_management										
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-010519/210					
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
			(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-2019-2709		
primavera_p6_enterprise_project_portfolio_management					
Improper Access Control	23-04-2019	4	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 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). CVE ID : CVE-2019-2701	N/A	A-ORA-PRIM-010519/211
database_server					

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
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

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
			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:H/UI:N/S:C/C:H/I:H/A:H). CVE ID : CVE-2019-2517		
Improper Access Control	23-04-2019	6	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 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:L/UI:N/S:U/C:H/I:H/A:H).	N/A	A-ORA-DATA-010519/214

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
			CVE ID : CVE-2019-2518		
N/A	23-04-2019	6	<p>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).</p> <p>CVE ID : CVE-2019-2571</p>	N/A	A-ORA-DATA-010519/215
Information Exposure	23-04-2019	5	<p>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 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</p>	N/A	A-ORA-DATA-010519/216

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
			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). CVE ID : CVE-2019-2582		

retail_convenience_store_back_office

Improper Access Control	23-04-2019	7.5	Vulnerability in the Oracle Retail Convenience Store Back Office component of Oracle Retail Applications (subcomponent: Level 3 Maintenance Functions). The supported version that is affected is 3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Convenience Store Back Office. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Convenience Store Back Office accessible data as well as unauthorized read access to a subset of Oracle Retail Convenience Store Back Office accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Convenience Store Back Office. CVSS 3.0 Base Score	N/A	A-ORA-RETA-010519/217
-------------------------	------------	-----	---	-----	-----------------------

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
			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_testing_suite

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-010519/218
-------------------------	------------	-----	--	-----	-----------------------

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					
			and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). CVE ID : CVE-2019-2557							
retail_point-of-service										
Improper Access Control	23-04-2019	7.5	Vulnerability in the Oracle Retail Point-of-Service component of Oracle Retail Applications (subcomponent: Infrastructure). Supported versions that are affected are 13.4, 14.0 and 14.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Point-of-Service. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Point-of-Service accessible data as well as unauthorized read access to a subset of Oracle Retail Point-of-Service accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Point-of-Service. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/	N/A	A-ORA-RETA-010519/219					
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					
			UI:N/S:U/C:L/I:L/A:L). CVE ID : CVE-2019-2558							
jd_edwards_enterpriseone_tools										
Improper Access Control	23-04-2019	4	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Tools 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-2019-2564	N/A	A-ORA-JD_E-010519/220					
jd_edwards_world_technical_foundation										
Improper Access Control	23-04-2019	5	Vulnerability in the JD Edwards World Technical Foundation component of Oracle JD Edwards Products (subcomponent: Service Enablement). Supported versions that are affected are A9.2, A9.3.1 and A9.4. Easily	N/A	A-ORA-JD_E-010519/221					
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					
			exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards World Technical Foundation. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards World Technical Foundation 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-2019-2565							
configurator										
Improper Access Control	23-04-2019	5	Vulnerability in the Oracle Configurator component of Oracle Supply Chain Products Suite (subcomponent: Active Model Generation). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle	N/A	A-ORA-CONF-010519/222					
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
			Configurator 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-2019-2567		

siebel_crm

Improper Access Control	23-04-2019	6.5	Vulnerability in the Siebel Core - Server BizLogic Script component of Oracle Siebel CRM (subcomponent: Integration - Scripting). The supported version that is affected is 19.3. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Siebel Core - Server BizLogic Script. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel Core - Server BizLogic Script accessible data as well as unauthorized read access to a subset of Siebel Core - Server BizLogic Script accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Siebel Core - Server BizLogic Script. CVSS 3.0 Base Score 4.7 (Confidentiality, Integrity and Availability impacts).	N/A	A-ORA-SIEB-010519/223
-------------------------	------------	-----	---	-----	-----------------------

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					
			CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L). CVE ID : CVE-2019-2570							
soa_suite										
Improper Access Control	23-04-2019	5	Vulnerability in the Oracle SOA Suite component of Oracle Fusion Middleware (subcomponent: Fabric Layer). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle SOA Suite 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). CVE ID : CVE-2019-2572	N/A	A-ORA-SOA_-010519/224					
autovue_3d_professional_advanced										
Information Exposure	23-04-2019	5	Vulnerability in the Oracle AutoVue 3D Professional Advanced component of Oracle Supply Chain Products Suite (subcomponent: Format Handling - 2D). Supported versions that are affected are 21.0.0 and 21.0.1. Easily	N/A	A-ORA-AUTO-010519/225					
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
			<p>exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle AutoVue 3D Professional Advanced. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle AutoVue 3D Professional Advanced 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).</p> <p>CVE ID : CVE-2019-2575</p>		

service_bus

Improper Access Control	23-04-2019	5	<p>Vulnerability in the Oracle Service Bus component of Oracle Fusion Middleware (subcomponent: Web Container). Supported versions that are affected are 11.1.1.9.0, 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 Service Bus. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Service Bus. CVSS 3.0 Base Score 5.3</p>	N/A	A-ORA-SERV-010519/226
-------------------------	------------	---	---	-----	-----------------------

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
			(Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2019-2576		

webcenter_sites

Improper Access Control	23-04-2019	5	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Advanced UI). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, 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 WebCenter Sites accessible data. CVSS 3.0 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N). CVE ID : CVE-2019-2578	N/A	A-ORA-WEBC-010519/227
Information Exposure	23-04-2019	4	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware	N/A	A-ORA-WEBC-010519/228

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
			(subcomponent: Advanced UI). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Sites 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-2019-2579		

isupplier_portal

Improper Access Control	23-04-2019	5.8	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	N/A	A-ORA-ISUP-010519/229
-------------------------	------------	-----	--	-----	-----------------------

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
			<p>while the vulnerability is in Oracle iSupplier Portal, 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 iSupplier Portal accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupplier Portal 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).</p> <p>CVE ID : CVE-2019-2583</p>		

business_intelligence_publisher

Information Exposure	23-04-2019	4	<p>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</p>	N/A	A-ORA-BUSI-010519/230
----------------------	------------	---	--	-----	-----------------------

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
			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

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
			<p>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).</p> <p>CVE ID : CVE-2019-2595</p>		
Improper Access Control	23-04-2019	4.9	<p>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</p>	N/A	A-ORA-BUSI-010519/232

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
			<p>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).</p> <p>CVE ID : CVE-2019-2601</p>		
Improper Access Control	23-04-2019	6.4	<p>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</p>	N/A	A-ORA-BUSI-010519/233

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
			<p>Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data as well as unauthorized read access to a subset of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).</p> <p>CVE ID : CVE-2019-2616</p>		

peoplesoft_enterprise_human_capital_management_talent_acquisition_manager

Improper Access Control	23-04-2019	5.8	<p>Vulnerability in the PeopleSoft Enterprise HCM Talent Acquisition Manager component of Oracle PeopleSoft Products (subcomponent: Job Opening). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Talent Acquisition Manager. Successful attacks require human interaction from a</p>	N/A	A-ORA-PEOP-010519/234
-------------------------	------------	-----	--	-----	-----------------------

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					
			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							
peoplesoft_enterprise_human_capital_management_candidate_gateway										
Improper Access Control	23-04-2019	5.8	Vulnerability in the PeopleSoft Enterprise HRMS component of Oracle PeopleSoft Products (subcomponent: Candidate Gateway). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker	N/A	A-ORA-PEOP-010519/235					
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
			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/UI:R/S:C/C:L/I:L/A:N). CVE ID : CVE-2019-2591		

email_center

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-010519/236
-------------------------	------------	-----	--	-----	-----------------------

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
			<p>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).</p> <p>CVE ID : CVE-2019-2600</p>		
Improper Access Control	23-04-2019	5.8	<p>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</p>	N/A	A-ORA-EMAI-010519/237

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
			<p>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).</p> <p>CVE ID : CVE-2019-2651</p>		
Improper Access Control	23-04-2019	5.8	<p>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</p>	N/A	A-ORA-EMAI-010519/238

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					
			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_fulfillment										
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-ONE- - 010519/239					
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
			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

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
			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-2019-2653		
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-	N/A	A-ORA-ONE- - 010519/241

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
			<p>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).</p> <p>CVE ID : CVE-2019-2654</p>		

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					
Improper Access Control	23-04-2019	4.3	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 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 update, insert or delete access to some of Oracle One-to-One Fulfillment 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-2019-2674	N/A	A-ORA-ONE-010519/242					
marketing										
Improper Access	23-04-2019	5.8	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- 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
Control			<p>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).</p> <p>CVE ID : CVE-2019-2604</p>		010519/243
Improper Access	23-04-2019	5.8	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- 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
Control			<p>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).</p> <p>CVE ID : CVE-2019-2664</p>		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- 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
Control			<p>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).</p> <p>CVE ID : CVE-2019-2670</p>		010519/245
Improper Access Control	23-04-2019	4.3	<p>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</p>	N/A	A-ORA-MARK-010519/246

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
			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-2019-2673		
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

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					
			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-2019-2677							
business_intelligence										
Information Exposure	23-04-2019	2.6	Vulnerability in the Oracle Business Intelligence Enterprise Edition component of Oracle Fusion Middleware (subcomponent: Web Catalog). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle	N/A	A-ORA-BUSI-010519/248					
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					
			Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N). CVE ID : CVE-2019-2605							
application_object_library										
Improper Access Control	23-04-2019	4.3	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-010519/249					
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					
			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/UI:R/S:C/C:N/I:L/A:N). CVE ID : CVE-2019-2621							
service_contracts										
Improper Access Control	23-04-2019	4.3	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, 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	N/A	A-ORA-SERV-010519/250					
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
			other than the attacker and while the vulnerability is in Oracle Service Contracts, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Service Contracts 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-2019-2622		

health_sciences_data_management_workbench

Improper Access 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 privileged attacker with network access via HTTP to compromise Oracle Health Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Health Sciences Data Management Workbench	N/A	A-ORA-HEAL-010519/251
-------------------------	------------	-----	--	-----	-----------------------

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
			accessible data as well as unauthorized read access to a subset of Oracle Health Sciences Data Management Workbench accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). CVE ID : CVE-2019-2629		

work_in_process

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-WORK-010519/252
-------------------------	------------	-----	--	-----	-----------------------

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
			(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_ledger

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): 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					
			UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2019-2638							
crm_technical_foundation										
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_-010519/254					
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
			(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

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
			(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

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
			(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

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
			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

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
			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-2019-2676		

trade_management

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 Management accessible data as well as unauthorized update, insert or delete	N/A	A-ORA-TRAD-010519/259
-------------------------	------------	-----	---	-----	-----------------------

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
			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

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
			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). CVE ID : CVE-2019-2641		
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	N/A	A-ORA-TRAD-010519/261

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
			<p>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).</p> <p>CVE ID : CVE-2019-2642</p>		
Improper Access Control	23-04-2019	5.8	<p>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</p>	N/A	A-ORA-TRAD-010519/262

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					
			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). CVE ID : CVE-2019-2643							
istore										
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 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
			<p>iStore, 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 iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore 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).</p> <p>CVE ID : CVE-2019-2652</p>		

interaction_center_intelligence

Improper Access Control	23-04-2019	5.8	<p>Vulnerability in the Oracle Interaction Center Intelligence component of Oracle E-Business Suite (subcomponent: Business Intelligence (OLTP)). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Interaction Center Intelligence. Successful attacks require human interaction from a person other than the attacker and</p>	N/A	A-ORA-INTE-010519/264
-------------------------	------------	-----	--	-----	-----------------------

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					
			while the vulnerability is in Oracle Interaction Center 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). CVE ID : CVE-2019-2655							
commerce_platform										
Improper Access Control	23-04-2019	5.8	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.	N/A	A-ORA-COMM-010519/265					
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
			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). CVE ID : CVE-2019-2659		
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

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					
			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). CVE ID : CVE-2019-2712							
knowledge_management										
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Knowledge Management component of Oracle E-Business Suite (subcomponent: Setup, Admin). 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	N/A	A-ORA-KNOW-010519/267					
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
			<p>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).</p> <p>CVE ID : CVE-2019-2660</p>		
Improper Access Control	23-04-2019	5.8	<p>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</p>	N/A	A-ORA-KNOW-010519/268

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					
			attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge accessible data as well as unauthorized read access to a subset of Oracle Knowledge 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-2019-2719							
territory_management										
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Territory Management component of Oracle E-Business Suite (subcomponent: Territory 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	N/A	A-ORA-TERR-010519/269					
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					
			unauthenticated attacker with network access via HTTP to compromise Oracle Territory Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Territory 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 Territory Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Territory 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-2019-2662							
advanced_outbound_telephony										
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-010519/270					
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
			<p>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).</p> <p>CVE ID : CVE-2019-2663</p>		
common_applications					

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
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Common Applications component of Oracle E-Business Suite (subcomponent: CRM User Management Framework). 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 Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, 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 Common Applications accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/	N/A	A-ORA-COMM-010519/271

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					
			UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2019-2665							
applications_framework										
Improper Access Control	23-04-2019	5.8	Vulnerability in the Oracle Applications Framework component of Oracle E-Business Suite (subcomponent: Attachments / File Upload). 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 Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, 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 Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.0 Base Score 8.2	N/A	A-ORA-APPL-010519/272					
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					
			(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-2019-2682							
mysql_connector/j										
Improper Input Validation	23-04-2019	3.5	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Connectors executes to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). CVE ID : CVE-2019-2692	N/A	A-ORA-MYSQ-010519/273					
peoplesoft_enterprise_elm_enterprise_learning_management										
Improper Access	23-04-2019	4	Vulnerability in the PeopleSoft Enterprise ELM component of Oracle	N/A	A-ORA-PEOP-					
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
Control			<p>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 PeopleSoft Enterprise ELM accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).</p> <p>CVE ID : CVE-2019-2700</p>		010519/274

hospitality_cruise_dining_room_management

Improper Input Validation	23-04-2019	6.4	<p>Vulnerability in the Oracle 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 Oracle Hospitality Cruise Dining Room Management. While</p>	N/A	A-ORA-HOSP-010519/275
---------------------------	------------	-----	--	-----	-----------------------

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
			<p>the vulnerability is in Oracle Hospitality Cruise Dining Room 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 Hospitality Cruise Dining Room Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Dining Room Management accessible data. CVSS 3.0 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).</p> <p>CVE ID : CVE-2019-2702</p>		

business_process_management_suite

Improper Access Control	23-04-2019	5.8	<p>Vulnerability in the Oracle 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</p>	N/A	A-ORA-BUSI-010519/276
-------------------------	------------	-----	--	-----	-----------------------

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					
			HTTP to compromise Oracle Business Process Management Suite. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Process Management Suite, 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 Business Process Management Suite accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Process Management Suite 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-2019-2706							
peoplesoft_enterprise_learning_management										
Improper Access Control	23-04-2019	5.8	Vulnerability in the PeopleSoft Enterprise ELM Enterprise Learning Management component of Oracle PeopleSoft Products (subcomponent: Application	N/A	A-ORA-PEOP-010519/277					
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
			<p>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).</p> <p>CVE ID : CVE-2019-2707</p>		

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
commerce_merchandising					
Improper Access Control	23-04-2019	6.4	<p>Vulnerability in the Oracle Commerce Merchandising component of Oracle Commerce (subcomponent: Asset Manager). 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 Merchandising. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Merchandising accessible data as well as unauthorized read access to a subset of Oracle Commerce Merchandising accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).</p> <p>CVE ID : CVE-2019-2713</p>	N/A	A-ORA-COMM-010519/278
data_integrator					
Information Exposure	23-04-2019	3.5	<p>Vulnerability in the Oracle Data Integrator component of Oracle Fusion Middleware (subcomponent: ODI Tools). Supported versions that are</p>	N/A	A-ORA-DATA-010519/279

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
			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). CVE ID : CVE-2019-2720		

weblogic_server

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-010519/280
-------------------------	------------	---	--	-----	-----------------------

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
			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): 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
			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/UI:N/S:U/C:H/I:L/A:N). CVE ID : CVE-2019-2618		
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

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
			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

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
			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). CVE ID : CVE-2019-2647		
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

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
			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). CVE ID : CVE-2019-2649	N/A	A-ORA-WEBL-010519/287
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	N/A	A-ORA-WEBL-010519/288

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
			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

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					
			UI:N/S:U/C:H/I:H/A:H). CVE ID : CVE-2019-2658							
e-business_suite										
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 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	N/A	A-ORA-E-BU-010519/290					
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
			(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_enterprise_peopletools

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
-------------------------	------------	-----	--	-----	-----------------------

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
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

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
			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): 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
			<p>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).</p> <p>CVE ID : CVE-2019-2597</p>		
Improper Access Control	23-04-2019	5.5	<p>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,</p>	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): 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
			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
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					
			Successful attacks 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 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-2019-2637							
database										
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	N/A	A-ORA-DATA-010519/297					
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					
			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-2019-2619							
Osticket										
osticket										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-04-2019	4.3	In osTicket before 1.12, XSS exists via /upload/file.php, /upload/scp/users.php?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	N/A	A-OST-OSTI-010519/298					
PHP										
php										
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_process_IFD_TAG function. This may lead to information disclosure or crash.	N/A	A-PHP-PHP-010519/299					
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
			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. CVE ID : CVE-2019-11035	N/A	A-PHP-PHP-010519/300
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 (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
			code. CVE ID : CVE-2019-11378		
Improper Neutralization 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://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3868	A-RED-KEYC-010519/305
rochoss					
rochoss					

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					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-04-2019	7.5	app/controllers/frontend/PostController.php in ROCCBOSS V2.2.1 has SQL injection via the Post:doReward score paramter, as demonstrated by the /do/reward/3 URI. CVE ID : CVE-2019-11362	N/A	A-ROC-ROCB-010519/306					
Sem-cms										
Semcms										
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-04-2019	6.5	An issue was discovered in SEMCMS 3.8. SEMCMS_Inquiry.php allows AID[] SQL Injection because the class.phpmailer.php inject_check_sql protection mechanism is incomplete. CVE ID : CVE-2019-11518	N/A	A-SEM-SEMC-010519/307					
Siemens										
simatic_cp443-1_opc_ua										
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 ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open	N/A	A-SIE-SIMA-010519/308					
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 Iniection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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) 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 Teleservice Adapter IE Basic (All versions), SIMATIC Teleservice Adapter IE Standard (All versions), SIMATIC WinAC RTX 2010 (All versions), SIMATIC WinCC Runtime Advanced		

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
			(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 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 V4.6 (All versions), SINAMICS S150 V4.7 (All versions), SINAMICS S150 V4.7 SP1 (All versions), SINAMICS S150 V4.8 (All		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		
simatic_ipc_diagmonitor					

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
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 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 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)	N/A	A-SIE-SIMA-010519/309

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
			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 Teleservice Adapter IE Basic (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 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		

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
			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 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		

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					
			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_s7-1500_software_controller										
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 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),	N/A	A-SIE-SIMA-010519/310					
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
			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) 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 Teleservice Adapter IE Basic (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		

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
			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 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 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),		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		
Improper Input Validation	17-04-2019	7.8	<p>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</p>	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): 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
			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 Mobile (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 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		

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
			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-plcsim_advanced

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 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 IPC DiagMonitor (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF182C (All versions), SIMATIC RF186C (All versions), SIMATIC RF188C (All versions),	N/A	A-SIE-SIMA-010519/312
---------------------------	------------	---	--	-----	-----------------------

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 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
			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) 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 Teleservice Adapter IE Basic (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 SP1 HF4), SINAMICS G150 V4.6 (All versions), SINAMICS G150 V4.7 (All		

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
			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 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 IRC (All versions). The webserver of the affected devices contains a vulnerability that may lead		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		

simatic_wincc_runtime_advanced

Improper Input Validation	17-04-2019	5	<p>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 ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2</p>	N/A	A-SIE-SIMA-010519/313
---------------------------	------------	---	--	-----	-----------------------

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
			(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 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) 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 Teleservice Adapter IE Basic (All versions), SIMATIC Teleservice Adapter IE Standard (All versions), SIMATIC WinAC RTX 2010 (All versions), SIMATIC WinCC Runtime Advanced (All versions), SIMOCODE		

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
			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 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 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),		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		
Improper Input	17-04-2019	7.8	A vulnerability has been identified in SIMATIC	N/A	A-SIE-SIMA-010519/314

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
Validation			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 Mobile (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 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		

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
			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		

sitop_manager

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 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	N/A	A-SIE-SITO-010519/315
---------------------------	------------	---	---	-----	-----------------------

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): 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
			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) 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 Teleservice Adapter IE Basic (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),		

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
			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 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 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		

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					
			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							
simatic_wincc_runtime_comfort										
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	A-SIE-SIMA-010519/316					
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
			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 Mobile (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 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		

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					
			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_wincc_runtime_hsp_comfort										
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 Mobile (All versions), SINEC-NMS (All versions), SINEMA Server (All versions), SINUMERIK OPC UA Server	N/A	A-SIE-SIMA-010519/317					
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					
			(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_wincc_runtime_mobile										
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-SIMA-010519/318					
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
			(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 Mobile (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 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		

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					
			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	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 Mobile (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-SINE-010519/319					
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	Patch	NCIIPC 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_server										
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-SINE-010519/320					
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
			<p>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 Mobile (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 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</p>		

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						
			vulnerability was known. CVE ID : CVE-2019-6575								
telecontrol_server_basic											
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 Mobile (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 network packets sent to affected devices on port 4840/tcp could allow an	N/A	A-SIE-TELE-010519/321						
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
			<p>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.</p> <p>CVE ID : CVE-2019-6575</p>		

spectrum_power_4

N/A	17-04-2019	7.5	<p>A vulnerability has been identified in Spectrum Power 4 (with Web Office Portal). An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected service. No user interaction is required to exploit this security vulnerability. Successful</p>	N/A	A-SIE-SPEC-010519/322
-----	------------	-----	---	-----	-----------------------

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
			exploitation of the security vulnerability compromises confidentiality, integrity or availability of the targeted system. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID : CVE-2019-6579		
siteserver					
siteserver_cms					
Unrestricted Upload of File with Dangerous Type	22-04-2019	6.5	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	N/A	A-SIT-SITE-010519/323
struktur					
libheif					
Use After Free	23-04-2019	6.8	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-LIBH-010519/324
supportcandy					
supportcandy					

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
Unrestricted Upload of File with Dangerous Type	18-04-2019	7.5	An Unrestricted File Upload Vulnerability in the SupportCandy plugin through 2.0.0 for WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension. CVE ID : CVE-2019-11223	N/A	A-SUP-SUPP-010519/325
tabslab					
mailcarrier					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2019	7.5	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	N/A	A-TAB-MAIL-010519/326
urllib3_project					
urllib3					
Improper Certificate Validation	18-04-2019	5	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.	N/A	A-URL-URLL-010519/327

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					
			CVE ID : CVE-2019-11324							
veronalabs										
wp_statistics										
Improper Neutralization 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	https://github.com/wp-statistics/wp-statistics/commit/5aec0a08680f0afea387267a8d1b9fbb3379247c	A-VER-WP_S-010519/328					
Verypdf										
verypdf										
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-04-2019	6.8	VeryPDF 4.1 has a Memory Overflow leading to Code Execution because pdfocx!CxlImageTIF::operator in pdfocx.ocx (used by pdfeditor.exe and pdfcmd.exe) is mishandled. CVE ID : CVE-2019-11493	N/A	A-VER-VERY-010519/329					
Vestacp										
control_panel										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-04-2019	4.3	Vesta Control Panel 0.9.8-23 allows XSS via a crafted URL. CVE ID : CVE-2019-9841	https://github.com/serghey-rodin/vesta/commit/c28c5d29a3c61bc8110c11349e3f2309cd537cfa	A-VES-CONT-010519/330					
W1.fi										
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	NCHPC ID					
hostapd										
Information Exposure	17-04-2019	4.3	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	https://w1.fi/security/2019-1/	A-W1.-HOST-010519/331					
Use of a Broken or Risky Cryptographic 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	https://w1.fi/security/2019-2/	A-W1.-HOST-010519/332					
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
			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 Authentication	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/2019-3/	A-W1.-HOST-010519/333
Improper Authentication	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/2019-4/	A-W1.-HOST-010519/334

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
			<p>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 prior to and including version 2.7 are affected.</p> <p>CVE ID : CVE-2019-9497</p>		
N/A	17-04-2019	6.8	<p>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</p>	https://w1.fi/security/2019-4/	A-W1.-HOST-010519/335

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					
			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 prior to and including version 2.7 are affected. CVE ID : CVE-2019-9498							
N/A	17-04-2019	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 prior to and including version 2.7 are affected. CVE ID : CVE-2019-9499	https://w1.fi/security/2019-4/	A-W1.-HOST-010519/336					
wpa_supplicant										
Information Exposure	17-04-2019	4.3	The implementations of SAE in hostapd and	https://w1.fi/security/2019-4/	A-W1.-WPA_-					
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
			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 Cryptographic 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/2019-2/	A-W1.- WPA_- 010519/338

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): 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
			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 Authentication	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/2019-3/	A-W1.-WPA_-010519/339
Improper Authentication	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/2019-4/	A-W1.-WPA_-010519/340

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
			<p>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 prior to and including version 2.7 are affected.</p> <p>CVE ID : CVE-2019-9497</p>		
N/A	17-04-2019	6.8	<p>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</p>	https://w1.fi/security/2019-4/	A-W1.-WPA_-010519/341

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
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					
			affected. 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-2019-9498							
N/A	17-04-2019	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 prior to and including version 2.7 are affected. CVE ID : CVE-2019-9499	https://w1.fi/security/2019-4/	A-W1.-WPA_-010519/342					
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-WAV-WAVP-010519/343					
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					
			"Conditional jump or move depends on uninitialised value" condition, which might allow attackers to cause a denial of service (application crash) via a DFF file that lacks valid sample-rate data. CVE ID : CVE-2019-11498							
wcms										
wcms										
Unrestricted Upload of File with Dangerous Type	20-04-2019	6.5	wcms/wex/finder/action.php in WCMS v0.3.2 has a Arbitrary File Upload Vulnerability via developer/finder because .php is a valid extension according to the fm_get_text_exts function. CVE ID : CVE-2019-11377	N/A	A-WCM-WCMS-010519/344					
whatsns										
whatsns										
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-04-2019	7.5	whatsns 4.0 allows index.php?question/ajaxadd.html title SQL injection. CVE ID : CVE-2019-11450	N/A	A-WHA-WHAT-010519/345					
Improper Neutralization of Special Elements used in an	22-04-2019	6.5	whatsns 4.0 allows index.php?inform/add.html qid SQL injection. CVE ID : CVE-2019-11451	N/A	A-WHA-WHAT-010519/346					
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 Iniection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-04-2019	6.5	whatsns 4.0 allows index.php?admin_category/remove.html cid[] SQL injection. CVE ID : CVE-2019-11452	N/A	A-WHA-WHAT-010519/347
wifi_ftp_server_project					
wifi_ftp_server					
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.wififtpservice/shared_prefs/com.medhaapps.wififtpservice_preferences.xml CVE ID : CVE-2019-11383	N/A	A-WIF-WIFI-010519/348
wordfence					
wordfence					
Improper Neutralization 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-WOR-WORD-010519/349

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
Scripting')					
zalora					
zalora					
N/A	22-04-2019	5	The Zalora application 6.15.1 for Android stores confidential information insecurely on the system (i.e. plain text), which allows a non-root user to find out the username/password of a valid user via /data/data/com.zalora.android/shared_prefs/login_data.xml. CVE ID : CVE-2019-11384	N/A	A-ZAL-ZALO-010519/350
Zohocorp					
servicedesk_plus					
Session Fixation	24-04-2019	6.5	Zoho ManageEngine ServiceDesk 9.3 allows session hijacking and privilege escalation because an established guest session is automatically converted into an established administrator session when the guest user enters the administrator username, with an arbitrary incorrect password, in an mc/ login attempt within a different browser tab. CVE ID : CVE-2019-10008	https://www.manageengine.com/products/service-desk/readme.html	A-ZOH-SERV-010519/351
manageengine_applications_manager					
Improper Neutralizatio	22-04-2019	10	An issue was discovered in Zoho ManageEngine	https://www.manageengi	A-ZOH-MANA-

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
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/products/applications_manager/security-updates/security-updates-cve-2019-11448.html	010519/352
Improper Neutralization 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. CVE ID : CVE-2019-11469	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2019-11469.html	A-ZOH-MANA-010519/353
Operating System					
ABB					
pm554-tp-eth_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

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
			CVE ID : CVE-2019-10953		
Canonical					
ubuntu_linux					
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_process_IFD_TAG function. This may lead to information disclosure or crash. CVE ID : CVE-2019-11034	N/A	O-CAN-UBUN-010519/355
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. CVE ID : CVE-2019-11035	N/A	O-CAN-UBUN-010519/356
Use After Free	18-04-2019	5	A use-after-free flaw was 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	N/A	O-CAN-UBUN-010519/357
centos-webpanel					
centos_web_panel					
Improper Neutralizatio	18-04-2019	3.5	CentOS-WebPanel.com (aka CWP) CentOS Web Panel	N/A	O-CEN-CENT-

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
n of Input During Web Page Generation ('Cross-site Scripting')			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		010519/358

Cisco

aironet_access_point_firmware

Improper Input Validation	17-04-2019	5.5	A vulnerability in the quality 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	O-CIS-AIRO-010519/359
Improper Authenticati	17-04-2019	7.2	A vulnerability in the CLI of Cisco Aironet Series Access	N/A	O-CIS-AIRO-

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
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 user-supplied 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

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
			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

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
			<p>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.</p> <p>CVE ID : CVE-2019-1835</p>		

ios_xr

Improper Access Control	17-04-2019	5	<p>A vulnerability in the TCP flags inspection feature for access control lists (ACLs) on Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to bypass protection offered by a configured ACL on an affected device. The vulnerability is due to incorrect processing of the ACL applied to an interface of an affected device when Cisco Express Forwarding load balancing using the 3-tuple hash algorithm is enabled. An attacker could exploit this vulnerability by sending traffic through an affected device that should otherwise be denied by the configured ACL. An exploit</p>	N/A	O-CIS-IOS_-010519/363
-------------------------	------------	---	---	-----	-----------------------

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
			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. CVE ID : CVE-2019-1711	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

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
			<p>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.</p> <p>CVE ID : CVE-2019-1712</p>		
Debian					
debian_linux					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-04-2019	4.3	<p>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 enumerable __proto__ property, it could extend the native Object.prototype.</p> <p>CVE ID : CVE-2019-11358</p>	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): 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
Dlink					
di-524_firmware					
Improper Neutralization 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, /smapi.htm, and /cgi-bin/smapi, as demonstrated by the cgi-bin/smapi RC parameter. CVE ID : CVE-2019-11017	N/A	O-DLI-DI-5-010519/367
Fedoraproject					
fedora					
Improper Authentication	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. CVE ID : CVE-2019-11234	N/A	O-FED-FEDO-010519/368
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-FED-FEDO-010519/369
Use After	18-04-2019	5	A use-after-free flaw was	N/A	O-FED-

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
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 prior to and including version 2.7 are affected. CVE ID : CVE-2019-9498	https://w1.fi/security/2019-4/	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/2019-4/	O-FED-FEDO-010519/372

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
			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 prior to and including version 2.7 are affected. CVE ID : CVE-2019-9499		

Google

android

N/A	19-04-2019	4.6	In updateAssistMenuItems of Editor.java, there is a possible escape from the Setup Wizard due to a missing permission check. This could lead to local escalation of privilege and FRP bypass with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0Android ID: A-120866126	https://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/373
-----	------------	-----	---	---	-----------------------

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
			CVE ID : CVE-2019-2026		
Out-of-bounds Write	19-04-2019	9.3	In floor0_inverse1 of floor0.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	https://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/374
Improper Input Validation	19-04-2019	9.3	In numerous hand-crafted functions in libmpeg2, NEON registers are not preserved. 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-120644655. CVE ID : CVE-2019-2028	https://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/375
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	https://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/376

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
			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. CVE ID : CVE-2019-2030	https://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/377
Out-of-bounds Write	19-04-2019	4.6	In rw_t3t_act_handle_check_ndef_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://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/378

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
			A-120502559. CVE ID : CVE-2019-2031		
Out-of-bounds Write	19-04-2019	4.6	In SetScanResponseData of ble_advertiser_hci_interface.cc, there is a possible out-of-bounds 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-8.0 Android-8.1 Android-9. Android ID: A-121145627. CVE ID : CVE-2019-2032	https://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/379
Use After Free	19-04-2019	4.6	In create_hdr of dnssd_clientstub.c, there is a possible use after free. 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-9. Android ID: A-121327565. CVE ID : CVE-2019-2033	https://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/380
Out-of-bounds Write	19-04-2019	6.8	In rw_i93_sm_read_ndef of rw_i93.cc, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege in the NFC process with no additional execution privileges needed.	https://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/381

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
			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://source.android.com/security/bulletin/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://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/383

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
			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. CVE ID : CVE-2019-2038	https://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/384
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://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/385
Out-of-	19-04-2019	4.7	In rw_i93_process_ext_sys_info	https://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-

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
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/bulletin/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://source.android.com/security/bulletin/2019-04-01	O-GOO-ANDR-010519/387

IBM

bladecenter_hs23_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.	N/A	O-IBM-BLAD-010519/388
---------------------------	------------	-----	---	-----	-----------------------

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					
			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_m4_hd_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-010519/391					
intelbras										
iwr_3000n_firmware										
Weak Password Recovery Mechanism for Forgotten	22-04-2019	4.3	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 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
Password			IP address, administrative authorization remains available to any client at that IP address, leading to complete control of the router. CVE ID : CVE-2019-11414		
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 Synchronization ('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

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
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					
m2_firmware					
Improper Neutralization 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-M2_F-010519/397
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 (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
Information Exposure	18-04-2019	5	An issue was discovered in Motorola CX2 1.01 and M2 1.01. The router opens TCP port 8010. Users can send hnap requests to this port 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 Neutralization 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					
Improper Neutralization 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 & CVE ID	Patch	NCIIPC ID
			192.168.51.1 address. CVE ID : CVE-2019-11320		
Information Exposure	18-04-2019	5	An issue was discovered in Motorola CX2 1.01 and M2 1.01. The router opens TCP port 8010. Users can send hnap requests to this port without authentication to obtain information such as the MAC addresses of connected client devices. CVE ID : CVE-2019-11321	N/A	O-MOT-CX2_-010519/403
Improper Neutralization 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-CX2_-010519/404

Oracle

solaris

Improper Access Control	23-04-2019	2.1	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	O-ORA-SOLA-010519/405
-------------------------	------------	-----	--	-----	-----------------------

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
			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		
Information Exposure	23-04-2019	5	Vulnerability in the Oracle Solaris component of Oracle 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). CVE ID : CVE-2019-2704	N/A	O-ORA-SOLA-010519/406
Phoenixcontact					
ilc_151_eth_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- 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
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-PHO-ILC_-010519/407
Redhat					
virtualization					
N/A	22-04-2019	4.3	A memory leak in archive_read_format_zip_cleanup in archive_read_support_format_zip.c in libarchive 3.3.4-dev allows remote attackers to cause a denial of service via a crafted ZIP file because of a HAVE_LZMA_H typo. NOTE: this only affects users who downloaded the development code from GitHub. Users of the product's official releases are unaffected. CVE ID : CVE-2019-11463	N/A	O-RED-VIRT-010519/408
enterprise_linux					
Improper Authentication	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	O-RED-ENTE-010519/409

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					
			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-electric										
modicon_m221_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_rf600r_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 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
			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 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) 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 Teleservice Adapter IE Basic		

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
			(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 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		

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
			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 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		

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
			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), SIMATIC WinCC Runtime Mobile (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 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	Patch	NCIIPC ID
			<p>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.</p> <p>CVE ID : CVE-2019-6575</p>		

simatic_s7-1500_firmware

Improper Input Validation	17-04-2019	5	<p>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 ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2</p>	N/A	O-SIE-SIMA-010519/414
---------------------------	------------	---	--	-----	-----------------------

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
			(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 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) 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 Teleservice Adapter IE Basic (All versions), SIMATIC Teleservice Adapter IE Standard (All versions), SIMATIC WinAC RTX 2010 (All versions), SIMATIC WinCC Runtime Advanced (All versions), SIMOCODE		

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
			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 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 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),		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		
Improper Input	17-04-2019	7.8	A vulnerability has been identified in SIMATIC	N/A	O-SIE-SIMA-010519/415

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
Validation			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 Mobile (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 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		

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
			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		

cp1604_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 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	N/A	O-SIE-CP16-010519/416
---------------------------	------------	---	---	-----	-----------------------

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
			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) 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 Teleservice Adapter IE Basic (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),		

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
			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 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 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		

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					
			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							
cp1616_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	N/A	O-SIE-CP16-010519/417					
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
			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 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 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) 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 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
			Teleservice Adapter IE Basic (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 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		

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
			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 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		

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					
			advisory publication no public exploitation of this security vulnerability was known. CVE ID : CVE-2019-6568							
simatic_cp343-1_advanced_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 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 IPC DiagMonitor (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF182C (All versions), SIMATIC RF186C (All versions), SIMATIC RF188C (All versions), SIMATIC RF600R (All	N/A	O-SIE-SIMA-010519/418					
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 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
			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) 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 Teleservice Adapter IE Basic (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 SP1 HF4), SINAMICS G150 V4.6 (All versions), SINAMICS G150 V4.7 (All versions), SINAMICS G150		

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
			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 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 IRC (All versions). The webserver of the affected devices contains a vulnerability that may lead to a denial-of-service		

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					
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>							
simatic_cp443-1_advanced_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 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	N/A	O-SIE-SIMA-010519/419					
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
			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 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) 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 Teleservice Adapter IE Basic (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),		

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 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 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 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		

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					
			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							
simatic_cp443-1_firmware										
Improper Input	17-04-2019	5	A vulnerability has been identified in CP1604 (All	N/A	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 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
Validation			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 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 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) V6 and below (All versions), SIMATIC S7-400 PN/DP V7		010519/420

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
			(incl. F) (All versions), SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC Teleservice Adapter IE Advanced (All versions), SIMATIC Teleservice Adapter IE Basic (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 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		

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
			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 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		

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					
			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_et_200_sp_open_controller_cpu_1515sp_pc2_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 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 IPC DiagMonitor (All versions), SIMATIC	N/A	O-SIE-SIMA-010519/421					
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
			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) 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 Teleservice Adapter IE Basic (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		

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
			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 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 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					
			(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_comfort_outdoor_panels_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),	N/A	O-SIE-SIMA-010519/422					
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
			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 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) 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 Teleservice Adapter IE Basic (All versions), SIMATIC Teleservice Adapter IE		

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
			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 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 V4.6 (All versions),		

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
			<p>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 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</p>		

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	NCHPC ID					
			known. CVE ID : CVE-2019-6568							
simatic_hmi_comfort_panels_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 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 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	N/A	O-SIE-SIMA-010519/423					
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
			Controller (All versions), SIMATIC S7-300 CPU family (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 Teleservice Adapter IE Basic (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 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),		

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
			<p>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 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</p>		

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					
			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_ktp400f_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 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-010519/424					
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
			(All versions), SIMATIC HMI KTP Mobile Panels KTP400F, 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) 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 Teleservice Adapter IE Basic (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 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
			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 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 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		

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					
			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							
simatic_hmi_ktp_mobile_panels_ktp700_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	N/A	O-SIE-SIMA-010519/425					
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 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
			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 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 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) V6 and below (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions), SIMATIC S7-PLCSIM Advanced (All versions),		

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
			SIMATIC Teleservice Adapter IE Advanced (All versions), SIMATIC Teleservice Adapter IE Basic (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 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		

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
			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 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		

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
			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_teleservice_adapter_ie_standard_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 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 IPC DiagMonitor (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF182C (All versions), SIMATIC RF186C	N/A	O-SIE-SIMA-010519/426
---------------------------	------------	---	---	-----	-----------------------

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
			(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) 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 Teleservice Adapter IE Basic (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 SP1 HF4), SINAMICS G150		

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
			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 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 IRC (All versions). The webserver of the affected		

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					
			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_winac_rtx_2010_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 ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6),	N/A	O-SIE-SIMA-010519/427					
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
			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 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) 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 Teleservice Adapter IE Basic (All versions), SIMATIC Teleservice Adapter IE Standard (All versions), SIMATIC WinAC RTX 2010 (All versions), SIMATIC		

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
			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 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 V4.6 (All versions), SINAMICS S150 V4.7 (All versions), SINAMICS S150 V4.7 SP1 (All versions),		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		

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_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 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 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	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	Description & CVE ID	Patch	NCIIPC ID
			(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 Teleservice Adapter IE Basic (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 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		

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
			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 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		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		

simocode_pro_v_pn_firmware

Improper Input Validation	17-04-2019	5	<p>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 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,</p>	N/A	O-SIE-SIMO-010519/429
---------------------------	------------	---	---	-----	-----------------------

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
			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) 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 Teleservice Adapter IE Basic (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		

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
			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 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 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		

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					
			(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							
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	N/A	O-SIE-SINA-010519/430					
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
			(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 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 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) 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		

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
			versions), SIMATIC Teleservice Adapter IE Basic (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 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		

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
			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 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		

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
			the device. At the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID : CVE-2019-6568		

sinamics_s210_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 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 IPC DiagMonitor (All versions), SIMATIC RF181-EIP (All versions), SIMATIC RF182C (All versions), SIMATIC RF186C (All versions), SIMATIC RF188C (All versions),	N/A	O-SIE-SINA-010519/431
---------------------------	------------	---	--	-----	-----------------------

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
			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) 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 Teleservice Adapter IE Basic (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 SP1 HF4), SINAMICS G150 V4.6 (All versions), SINAMICS G150 V4.7 (All		

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
			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 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 IRC (All versions). The webserver of the affected devices contains a vulnerability that may lead		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		

sitop_psu8600_firmware

Improper Input Validation	17-04-2019	5	<p>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 ET 200 SP Open Controller CPU 1515SP PC (All versions < V2.1.6), SIMATIC ET 200 SP Open Controller CPU 1515SP PC2</p>	N/A	O-SIE-SITO-010519/432
---------------------------	------------	---	--	-----	-----------------------

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
			(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 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) 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 Teleservice Adapter IE Basic (All versions), SIMATIC Teleservice Adapter IE Standard (All versions), SIMATIC WinAC RTX 2010 (All versions), SIMATIC WinCC Runtime Advanced (All versions), SIMOCODE		

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
			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 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 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),		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		
sitop_ups1600_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- 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), 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 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 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)	N/A	O-SIE-SITO-010519/433

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
			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 Teleservice Adapter IE Basic (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 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		

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
			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 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		

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
			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_ktp700f_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 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),	N/A	O-SIE-SIMA-010519/434
---------------------------	------------	---	---	-----	-----------------------

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
			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) 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 Teleservice Adapter IE Basic (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		

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
			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 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 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),		

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					
			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							
simatic_hmi_ktp_mobile_panels_ktp900_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-010519/435					
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
			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 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) 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 Teleservice Adapter IE Basic		

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
			(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 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		

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
			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 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		

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					
			public exploitation of this security vulnerability was known. CVE ID : CVE-2019-6568							
simatic_hmi_ktp_mobile_panels_ktp900f_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 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 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	N/A	O-SIE-SIMA-010519/436					
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 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
			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) 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 Teleservice Adapter IE Basic (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 SP1 HF4), SINAMICS G150 V4.6 (All versions), SINAMICS G150 V4.7 (All versions), SINAMICS G150 V4.7 SP1 (All versions),		

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
			<p>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 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 IRC (All versions). The webserver of the affected devices contains a vulnerability that may lead to a denial-of-service condition. An attacker may</p>		

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					
			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_rf181-eip_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 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" &	N/A	O-SIE-SIMA-010519/437					
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): 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
			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 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) 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 Teleservice Adapter IE Basic (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		

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
			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 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 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		

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					
			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							
simatic_rf182c_firmware										
Improper Input	17-04-2019	5	A vulnerability has been identified in CP1604 (All versions), CP1616 (All	N/A	O-SIE-SIMA-010519/438					
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
Validation			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 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 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) V6 and below (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions),		

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
			SIMATIC S7-PLCSIM Advanced (All versions), SIMATIC Teleservice Adapter IE Advanced (All versions), SIMATIC Teleservice Adapter IE Basic (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 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 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
			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 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		

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	NCHPC ID					
			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_rf185c_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 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 IPC DiagMonitor (All versions), SIMATIC RF181-EIP (All versions),	N/A	O-SIE-SIMA-010519/439					
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
			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) 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 Teleservice Adapter IE Basic (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		

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
			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 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 IRC		

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					
			(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_rf186c_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 ET 200 SP Open	N/A	O-SIE-SIMA-010519/440					
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
			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 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) 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 Teleservice Adapter IE Basic (All versions), SIMATIC Teleservice Adapter IE Standard (All versions),		

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
			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 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 V4.6 (All versions), SINAMICS S150 V4.7 (All		

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
			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		

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	NCHPC ID					
			known. CVE ID : CVE-2019-6568							
simatic_teleservice_adapter_ie_advanced_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 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 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	N/A	O-SIE-SIMA-010519/441					
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
			Controller (All versions), SIMATIC S7-300 CPU family (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 Teleservice Adapter IE Basic (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 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),		

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
			<p>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 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</p>		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		

simatic_teleservice_adapter_ie_basic_firmware

Improper Input Validation	17-04-2019	5	<p>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 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"</p>	N/A	O-SIE-SIMA-010519/442
---------------------------	------------	---	--	-----	-----------------------

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
			(All versions), SIMATIC HMI KTP Mobile Panels KTP400F, 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) 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 Teleservice Adapter IE Basic (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 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
			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 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 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		

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					
			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							
simatic_s7-1500f_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	N/A	O-SIE-SIMA-010519/443					
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
			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 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 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) V6 and below (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions), SIMATIC S7-PLCSIM Advanced (All versions),		

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
			SIMATIC Teleservice Adapter IE Advanced (All versions), SIMATIC Teleservice Adapter IE Basic (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 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		

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
			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 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		

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
			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), SIMATIC WinCC Runtime Mobile (All versions), SINEC-NMS (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	Description & CVE ID	Patch	NCIIPC ID					
			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_s7-1500s_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 ET 200 SP Open	N/A	O-SIE-SIMA-010519/445					
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 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
			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 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) 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 Teleservice Adapter IE Basic (All versions), SIMATIC Teleservice Adapter IE Standard (All versions),		

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
			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 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 V4.6 (All versions), SINAMICS S150 V4.7 (All		

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
			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		

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
			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 Mobile (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 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	Description & CVE ID	Patch	NCIIPC ID
			<p>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.</p> <p>CVE ID : CVE-2019-6575</p>		

simatic_s7-1500t_firmware

Improper Input Validation	17-04-2019	5	<p>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 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" &</p>	N/A	O-SIE-SIMA-010519/447
---------------------------	------------	---	--	-----	-----------------------

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
			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 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) 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 Teleservice Adapter IE Basic (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		

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
			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 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 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		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		
Improper Input Validation	17-04-2019	7.8	<p>A vulnerability has been identified in SIMATIC CP443-1 OPC UA (All versions), SIMATIC ET 200</p>	N/A	O-SIE-SIMA-010519/448

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
			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 Mobile (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 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		

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
			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_s7-300_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 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 IPC DiagMonitor	N/A	O-SIE-SIMA-010519/449
---------------------------	------------	---	---	-----	-----------------------

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
			(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) 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 Teleservice Adapter IE Basic (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),		

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
			SINAMICS G130 V5.1 (All 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 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		

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					
			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_s7-400_pn/dp_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	N/A	O-SIE-SIMA-010519/450					
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
			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 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) 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 Teleservice Adapter IE Basic (All versions), SIMATIC		

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
			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 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		

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
			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 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		

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					
			security vulnerability was known. CVE ID : CVE-2019-6568							
simatic_s7-400_pn_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 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 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),	N/A	O-SIE-SIMA-010519/451					
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 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
			SIMATIC S7-1500 Software Controller (All versions), SIMATIC S7-300 CPU family (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 Teleservice Adapter IE Basic (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 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		

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
			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 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		

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
			<p>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.</p> <p>CVE ID : CVE-2019-6568</p>		

simatic_rf188c_firmware

Improper Input Validation	17-04-2019	5	<p>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 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</p>	N/A	O-SIE-SIMA-010519/452
---------------------------	------------	---	--	-----	-----------------------

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 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
			HMI Comfort Panels 4" - 22" (All versions), SIMATIC HMI KTP Mobile Panels KTP400F, 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) 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 Teleservice Adapter IE Basic (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 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
			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 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 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		

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
			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

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
			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 Mobile (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 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		

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					
			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							
tim_1531_irc_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 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 IPC DiagMonitor (All versions), SIMATIC	N/A	O-SIE-TIM_-010519/454					
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
			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) 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 Teleservice Adapter IE Basic (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		

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
			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 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 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					
			(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_cp443-1_opc_ua_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	N/A	O-SIE-SIMA-010519/455					
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
			(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 Mobile (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 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		

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					
			the time of advisory publication no public exploitation of this security vulnerability was known. CVE ID : CVE-2019-6575							
simatic_et_200_open_controller_cpu_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 Mobile (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	O-SIE-SIMA-010519/456					
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					
			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_ipc_diagmonitor_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	N/A	O-SIE-SIMA-010519/457					
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
			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 Mobile (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 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		

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					
			vulnerability was known. CVE ID : CVE-2019-6575							
simatic_net_pc_software_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 Mobile (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 network packets sent to affected devices on port 4840/tcp could allow an	N/A	O-SIE-SIMA-010519/458					
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					
			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							
6ed1052-1cc01-0ba8_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-SIE-6ED1-010519/459					
6es7211-1ae40-0xb0_firmware										
Uncontrolled Resource Consumption	17-04-2019	5	ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO - Programmable Logic Controllers, multiple versions. Researchers have	N/A	O-SIE-6ES7-010519/460					
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
			found some controllers are susceptible to a denial-of-service attack due to a flood of network packets. CVE ID : CVE-2019-10953		
6es7314-6eh04-0ab0_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-SIE-6ES7-010519/461
Trendnet					
tv-ip110wn_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	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 using the languse parameter with a long string. This affects 1.2.2 build 28, 64, 65, and 68. CVE ID : CVE-2019-11417	N/A	O-TRE-TV-I-010519/462
tew-632brp_firmware					
Improper Restriction of	22-04-2019	7.5	apply.cgi on the TRENDnet TEW-632BRP 1.010B32 router has a buffer overflow	N/A	O-TRE-TEW-010519/463

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					
Operations within the Bounds of a Memory Buffer			via long strings to the SOAPACTION:HNAP1 interface. CVE ID : CVE-2019-11418							
Wago										
bacnet/ip_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-WAG-BACN-010519/464					
ethernet_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-WAG-ETHE-010519/465					
knx_ip_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-	N/A	O-WAG-KNX_-010519/466					
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					
			service attack due to a flood of network packets. CVE ID : CVE-2019-10953							
pfc100_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-WAG-PFC1-010519/467					
xinruidz										
sundray_wan_controller_firmware										
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 port 22345) and escalate to root (because the password for root is the WebUI admin password concatenated with a static string). CVE ID : CVE-2019-9160	N/A	O-XIN-SUND-010519/468					
Improper Neutralization 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-010519/469					
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
Injection')			metacharacters in the nginx_webconsole.php Cookie header can be used to read an etc/config/wac/wns_cfg_admin_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		
Hardware					
Intel					
-					
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/content/www/us/en/security-center/advisory/intel-sa-00238.html	H-INT---010519/470

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.										