National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 - 31 Jan 2020 Vol. 07 No. 02

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
77bank					
77_bank					
Improper Certificate Validation	28-01-2020	5.8	Android App 'MyPallete' and some of the Android banking applications based on 'MyPallete' do not verify X.509 certificates from servers, and also do not properly validate certificates with host-mismatch, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2020-5523**	N/A	A-77B-77_B-030220/1
adive					
framework					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	Adive Framework 2.0.8 has admin/user/add userUsername XSS. **CVE ID : CVE-2020-7989**	N/A	A-ADI-FRAM-030220/2
Improper Neutralization of Input During Web Page Generation	26-01-2020	4.3	Adive Framework 2.0.8 has admin/user/add userName XSS. **CVE ID : CVE-2020-7990**	N/A	A-ADI-FRAM-030220/3

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Cross-Site Request Forgery (CSRF)	26-01-2020	6.8	Adive Framework 2.0.8 has admin/config CSRF to change the Administrator password. **CVE ID : CVE-2020-7991**	N/A	A-ADI-FRAM-030220/4
Adobe					
illustrator_cc					
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-01-2020	9.3	Adobe Illustrator CC versions 24.0 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3710**	https://helpx.adobe.com/security/products/illustrator/apsb20-03.html	A-ADO-ILLU-030220/5
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-01-2020	9.3	Adobe Illustrator CC versions 24.0 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3711**	https://helpx.adobe.com/security/products/illustrator/apsb20-03.html	A-ADO-ILLU-030220/6
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-01-2020	9.3	Adobe Illustrator CC versions 24.0 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3712**	https://helpx.adobe.com/security/products/illustrator/apsb20-03.html	A-ADO-ILLU-030220/7
Improper Restriction of Operations within the Bounds of a	29-01-2020	9.3	Adobe Illustrator CC versions 24.0 and earlier have a memory corruption vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/illustrator/apsb20-	A-ADO-ILLU-030220/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			arbitrary code execution. **CVE ID : CVE-2020-3713**	03.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-01-2020	9.3	Adobe Illustrator CC versions 24.0 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3714**	https://helpx.adobe.com/security/products/illustrator/apsb20-03.html	A-ADO-ILLU-030220/9
amcrest					
web_server					
Improper Authentication	18-01-2020	5	An issue was discovered in Amcrest Web Server 2.520.AC00.18.R 2017-06-29 WEB 3.2.1.453504. The login page responds with JavaScript when one tries to authenticate. An attacker who changes the result parameter (to true) in this JavaScript code can bypass authentication and achieve limited privileges (ability to see every option but not modify them). **CVE ID : CVE-2020-7222**	N/A	A-AMC-WEB_-030220/10
Apache					
spamassassin					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-01-2020	9.3	A command execution issue was found in Apache SpamAssassin prior to 3.4.3. Carefully crafted nefarious rule configuration (.cf) files can be configured to run system commands similar to CVE-2018-11805. With this bug unpatched, exploits	https://bz.apache.org/SpamAssassin/show_bug.cgi?id=7648	A-APA-SPAM-030220/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be injected in a number of scenarios including the same privileges as spamd is run which may be elevated though doing so remotely is difficult. In addition to upgrading to SA 3.4.4, we again recommend that users should only use update channels or 3rd party .cf files from trusted places. If you cannot upgrade, do not use 3rd party rulesets, do not use sa-compile and do not run spamd as an account with elevated privileges. **CVE ID : CVE-2020-1930**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-01-2020	9.3	A command execution issue was found in Apache SpamAssassin prior to 3.4.3. Carefully crafted nefarious Configuration (.cf) files can be configured to run system commands similar to CVE-2018-11805. This issue is less stealthy and attempts to exploit the issue will throw warnings. Thanks to Damian Lukowski at credativ for reporting the issue ethically. With this bug unpatched, exploits can be injected in a number of scenarios though doing so remotely is difficult. In addition to upgrading to SA 3.4.4, we again recommend that users should only use update channels or 3rd party .cf files from trusted	https://bz.apache.org/SpamAssassin/show_bug.cgi?id=7784	A-APA-SPAM-030220/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			places. **CVE ID : CVE-2020-1931**		
nifi					
Information Exposure	28-01-2020	5	An information disclosure vulnerability was found in Apache NiFi 1.10.0. The sensitive parameter parser would log parsed values for debugging purposes. This would expose literal values entered in a sensitive property when no parameter was present. **CVE ID : CVE-2020-1928**	https://nifi.apache.org/security.html#CVE-2020-1928	A-APA-NIFI-030220/13
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-01-2020	4.3	A XSS vulnerability was found in Apache NiFi 1.0.0 to 1.10.0. Malicious scripts could be injected to the UI through action by an unaware authenticated user in Firefox. Did not appear to occur in other browsers. **CVE ID : CVE-2020-1933**	https://nifi.apache.org/security.html#CVE-2020-1933	A-APA-NIFI-030220/14
superset					
Information Exposure	28-01-2020	4	An information disclosure issue was found in Apache Superset 0.34.0, 0.34.1, 0.35.0, and 0.35.1. Authenticated Apache Superset users are able to retrieve other users' information, including hashed passwords, by accessing an unused and undocumented API endpoint on Apache Superset. **CVE ID : CVE-2020-1932**	N/A	A-APA-SUPE-030220/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
apt-cacher-ng_project					
apt-cacher-ng					
Information Exposure	21-01-2020	2.1	apt-cacher-ng through 3.3 allows local users to obtain sensitive information by hijacking the hardcoded TCP port. The /usr/lib/apt-cacher-ng/acngtool program attempts to connect to apt-cacher-ng via TCP on localhost port 3142, even if the explicit SocketPath=/var/run/apt-cacher-ng/socket command-line option is passed. The cron job /etc/cron.daily/apt-cacher-ng (which is active by default) attempts this periodically. Because 3142 is an unprivileged port, any local user can try to bind to this port and will receive requests from acngtool. There can be sensitive data in these requests, e.g., if AdminAuth is enabled in /etc/apt-cacher-ng/security.conf. This sensitive data can leak to unprivileged local users that manage to bind to this port before the apt-cacher-ng daemon can. **CVE ID : CVE-2020-5202**	N/A	A-APT-APT--030220/16
ashikagabank					
ashigin					
Improper Certificate	28-01-2020	5.8	Android App 'MyPallete' and some of the Android	N/A	A-ASH-ASHI-030220/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			banking applications based on 'MyPallete' do not verify X.509 certificates from servers, and also do not properly validate certificates with host-mismatch, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2020-5523**		
bearftp_project					
bearftp					
Uncontrolled Resource Consumption	29-01-2020	5	BearFTP before 0.2.0 allows remote attackers to achieve denial of service via a large volume of connections to the PASV mode port. **CVE ID : CVE-2020-8416**	https://github.com/kolya5544/BearFTP/blob/0.2.0/CHANGELOG.txt, https://github.com/kolya5544/BearFTP/commit/9965337f9d4c0325e4aab324dcd485e4cbb7b428, https://github.com/kolya5544/BearFTP/releases/tag/0.2.0	A-BEA-BEAR-030220/18
Cacti					
cacti					
Improper Neutralization of Input	16-01-2020	4.3	Cacti 1.2.8 has stored XSS in data_sources.php, color_templates_item.php,	N/A	A-CAC-CACT-030220/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			graphs.php, graph_items.php, lib/api_automation.php, user_admin.php, and user_group_admin.php, as demonstrated by the description parameter in data_sources.php (a raw string from the database that is displayed by $header to trigger the XSS). **CVE ID : CVE-2020-7106**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-01-2020	9	Cacti 1.2.8 allows Remote Code Execution (by privileged users) via shell metacharacters in the Performance Boost Debug Log field of poller_automation.php. OS commands are executed when a new poller cycle begins. The attacker must be authenticated, and must have access to modify the Performance Settings of the product. **CVE ID : CVE-2020-7237**	N/A	A-CAC-CACT-030220/20
Cisco					
jabber_guest					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Jabber Guest could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected	N/A	A-CIS-JABB-030220/21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability exists because the web-based management interface of the affected device does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or to access sensitive, browser-based information. This vulnerability affects Cisco Jabber Guest releases 11.1(2) and earlier. **CVE ID : CVE-2020-3136**		
email_security_appliance					
Improper Input Validation	26-01-2020	6.4	A vulnerability in the zip decompression engine of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of zip files. An attacker could exploit this vulnerability by sending an email message with a crafted zip-compressed attachment. A successful exploit could trigger a restart of the	N/A	A-CIS-EMAI-030220/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			content-scanning process, causing a temporary DoS condition. This vulnerability affects Cisco AsyncOS Software for Cisco ESA releases earlier than 13.0. **CVE ID : CVE-2020-3134**		
webex_teams					
Uncontrolled Resource Consumption	26-01-2020	4	A vulnerability in the Cisco Webex Teams client for Windows could allow an authenticated, remote attacker to cause the client to crash, resulting in a denial of service (DoS) condition. The attacker needs a valid developer account to exploit this vulnerability. The vulnerability is due to insufficient input validation when processing received adaptive cards. The attacker could exploit this vulnerability by sending an adaptive card with malicious content to an existing user of the Cisco Webex Teams client for Windows. A successful exploit could allow the attacker to cause the targeted user's client to crash continuously. This vulnerability was introduced in Cisco Webex Teams client for Windows Release 3.0.13131. **CVE ID : CVE-2020-3131**	N/A	A-CIS-WEBE-030220/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
webex_meetings_online					
Missing Authenticati on for Critical Function	26-01-2020	5	A vulnerability in Cisco Webex Meetings Suite sites and Cisco Webex Meetings Online sites could allow an unauthenticated, remote attendee to join a password-protected meeting without providing the meeting password. The connection attempt must initiate from a Webex mobile application for either iOS or Android. The vulnerability is due to unintended meeting information exposure in a specific meeting join flow for mobile applications. An unauthorized attendee could exploit this vulnerability by accessing a known meeting ID or meeting URL from the mobile device’s web browser. The browser will then request to launch the device’s Webex mobile application. A successful exploit could allow the unauthorized attendee to join the password-protected meeting. The unauthorized attendee will be visible in the attendee list of the meeting as a mobile attendee. Cisco has applied updates that address this vulnerability and no user action is required. This	N/A	A-CIS-WEBE-030220/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Cisco Webex Meetings Suite sites and Cisco Webex Meetings Online sites releases earlier than 39.11.5 and 40.1.3. **CVE ID : CVE-2020-3142**		
unity_connection					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	3.5	A vulnerability in the web-based management interface of Cisco Unity Connection Software could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by providing crafted data to a specific field within the interface. A successful exploit could allow the attacker to store an XSS attack within the interface. This stored XSS attack would then be executed on the system of any user viewing the attacker-supplied data element. **CVE ID : CVE-2020-3129**	N/A	A-CIS-UNIT-030220/25
application_policy_infrastructure_controller					
Improper Input Validation	26-01-2020	5	A vulnerability in the out of band (OOB) management interface IP table rule programming for Cisco Application Policy	N/A	A-CIS-APPL-030220/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure Controller (APIC) could allow an unauthenticated, remote attacker to bypass configured deny entries for specific IP ports. These IP ports would be permitted to the OOB management interface when, in fact, the packets should be dropped. The vulnerability is due to the configuration of specific IP table entries for which there is a programming logic error that results in the IP port being permitted. An attacker could exploit this vulnerability by sending traffic to the OOB management interface on the targeted device. A successful exploit could allow the attacker to bypass configured IP table rules to drop specific IP port traffic. The attacker has no control over the configuration of the device itself. This vulnerability affects Cisco APIC releases prior to the first fixed software Release 4.2(3j). **CVE ID : CVE-2020-3139**		
codecov					
nodejs_uploader					
Improper Neutralization of Special Elements in Output Used	25-01-2020	6.5	Codecov npm module before 3.6.2 allows remote attackers to execute arbitrary commands via the "gcov-args" argument.	N/A	A-COD-NODE-030220/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			**CVE ID : CVE-2020-7596**		
Codepeople					
calculated_fields_form					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-01-2020	3.5	The Calculated Fields Form plugin through 1.0.353 for WordPress suffers from multiple Stored XSS vulnerabilities present in the input forms. These can be exploited by an authenticated user. **CVE ID : CVE-2020-7228**	N/A	A-COD-CALC-030220/28
Codesys					
control_for_plcnext					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-CONT-030220/29
control_for_beaglebone					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef	A-COD-CONT-030220/30

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				7592d&download=	
control_for_empc-a\/imx6					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-CONT-030220/31
control_for_iot2000					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-CONT-030220/32
control_for_linux					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-CONT-030220/33
control_for_pfc100					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-CONT-030220/34
control_for_pfc200					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-CONT-030220/35
control_for_raspberry_pi					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-CONT-030220/36
control_rte					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow	https://customers.codesys.com/index.ph	A-COD-CONT-030220/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	p?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	
control_runtime_system_toolkit					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-CONT-030220/38
control_win					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-CONT-030220/39
hmi					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=3	A-COD-HMI-030220/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. **CVE ID : CVE-2020-7052**	3f948eed0c2fd69d238d9515779be337ef7592d&download=	
simulation_runtime					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-SIMU-030220/41
gateway					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	A-COD-GATE-030220/42
safety_sil2					
Uncontrolled Resource Consumption	24-01-2020	4	CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition. **CVE ID : CVE-2020-7052**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef	A-COD-SAFE-030220/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				7592d&download=	
ctfd					
ctfd					
Weak Password Recovery Mechanism for Forgotten Password	23-01-2020	6.8	Incorrect username validation in the registration process of CTFd v2.0.0 - v2.2.2 allows an attacker to take over an arbitrary account if the username is known and emails are enabled on the CTFd instance. To exploit the vulnerability, one must register with a username identical to the victim's username, but with white space inserted before and/or after the username. This will register the account with the same username as the victim. After initiating a password reset for the new account, CTFd will reset the victim's account password due to the username collision. **CVE ID : CVE-2020-7245**	N/A	A-CTF-CTFD-030220/44
django-user-sessions_project					
django-user-sessions					
Inadequate Encryption Strength	24-01-2020	4	In Django User Sessions (django-user-sessions) before 1.7.1, the views provided allow users to terminate specific sessions. The session key is used to identify sessions, and thus included in the rendered HTML. In itself this is not a	https://github.com/Bouke/django-user-sessions/security/advisories/GHSA-5fq8-3q2f-4m5g	A-DJA-DJAN-030220/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			problem. However if the website has an XSS vulnerability, the session key could be extracted by the attacker and a session takeover could happen. **CVE ID : CVE-2020-5224**		
Dolibarr					
dolibarr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Dolibarr 10.0.6 allow remote attackers to inject arbitrary web script or HTML via the (1) label[libelle] parameter to the /htdocs/admin/dict.php?id=3 page; the (2) name[constname] parameter to the /htdocs/admin/const.php?mainmenu=home page; the (3) note[note] parameter to the /htdocs/admin/dict.php?id=10 page; the (4) zip[MAIN_INFO_SOCIETE_ZIP] or email[mail] parameter to the /htdocs/admin/company.php page; the (5) url[defaulturl], field[defaultkey], or value[defaultvalue] parameter to the /htdocs/admin/defaultvalues.php page; the (6) key[transkey] or key[transvalue] parameter	N/A	A-DOL-DOLI-030220/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the /htdocs/admin/translation.php page; or the (7) [main_motd] or [main_home] parameter to the /htdocs/admin/ihm.php page. **CVE ID : CVE-2020-7994**		
Improper Authentication	26-01-2020	10	The htdocs/index.php?mainmenu=home login page in Dolibarr 10.0.6 allows an unlimited rate of failed authentication attempts. **CVE ID : CVE-2020-7995**	N/A	A-DOL-DOLI-030220/47
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	htdocs/user/passwordforgotten.php in Dolibarr 10.0.6 allows XSS via the Referer HTTP header. **CVE ID : CVE-2020-7996**	N/A	A-DOL-DOLI-030220/48
elementor					
elementor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-01-2020	3.5	The Elementor plugin before 2.8.5 for WordPress suffers from a reflected XSS vulnerability on the elementor-system-info page. These can be exploited by targeting an authenticated user. **CVE ID : CVE-2020-8426**	N/A	A-ELE-ELEM-030220/49
elementor_page_builder					
N/A	22-01-2020	7.5	The Elementor Page Builder plugin before 2.8.4 for	N/A	A-ELE-ELEM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WordPress does not sanitize data during creation of a new template. **CVE ID : CVE-2020-7109**		030220/50
etoilewebdesign					
ultimate_faq					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-01-2020	4.3	The Ultimate FAQ plugin before 1.8.30 for WordPress allows XSS via Display_FAQ to Shortcodes/DisplayFAQs.php. **CVE ID : CVE-2020-7107**	N/A	A-ETO-ULTI-030220/51
evoko					
home					
Information Exposure Through an Error Message	19-01-2020	5	Evoko Home 1.31 devices provide different error messages for failed login requests depending on whether the username is valid. **CVE ID : CVE-2020-7231**	N/A	A-EVO-HOME-030220/52
Information Exposure	19-01-2020	5	Evoko Home 1.31 devices allow remote attackers to obtain sensitive information (such as usernames and password hashes) via a WebSocket request, as demonstrated by the sockjs/224/uf1psgff/websocket URI at a wss:// URL. **CVE ID : CVE-2020-7232**	N/A	A-EVO-HOME-030220/53
fujixerox					
netprint					
Improper Certificate	27-01-2020	5.8	The netprint App for iOS 3.2.3 and earlier does not	N/A	A-FUJ-NETP-030220/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			verify X.509 certificates from servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2020-5520**		
easy_netprint					
Improper Certificate Validation	27-01-2020	5.8	The kantan netprint App for iOS 2.0.2 and earlier does not verify X.509 certificates from servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2020-5521**	N/A	A-FUJ-EASY-030220/55
Improper Certificate Validation	27-01-2020	5.8	The kantan netprint App for Android 2.0.3 and earlier does not verify X.509 certificates from servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2020-5522**	N/A	A-FUJ-EASY-030220/56
gallagher					
command_centre					
Information Exposure	20-01-2020	2.1	An issue was discovered in Gallagher Command Centre 7.x before 7.90.991(MR5), 8.00 before 8.00.1161(MR5), and 8.10 before 8.10.1134(MR4). External system	N/A	A-GAL-COMM-030220/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration data (used for third party integrations such as DVR systems) were logged in the Command Centre event trail. Any authenticated operator with the 'view events' privilege could see the full configuration, including cleartext usernames and passwords, under the event details of a Modified DVR System event. **CVE ID : CVE-2020-7215**		
grin					
grin					
Improper Input Validation	21-01-2020	5	Grin through 2.1.1 has Insufficient Validation. **CVE ID : CVE-2020-6638**	https://github.com/mimblewimble/grin-security/blob/master/CVEs/CVE-2020-6638.md	A-GRI-GRIN-030220/58
hashicorp					
vault					
Information Exposure	23-01-2020	4.3	HashiCorp Vault Enterprise 0.11.0 through 1.3.1 fails, in certain circumstances, to revoke dynamic secrets for a mount in a deleted namespace. Fixed in 1.3.2. **CVE ID : CVE-2020-7220**	https://github.com/hashicorp/vault/blob/master/CHANGELOG.md#132-january-22nd-2020	A-HAS-VAUL-030220/59
hokkaidobank					
dogin					
Improper Certificate	28-01-2020	5.8	Android App 'MyPallete' and some of the Android	N/A	A-HOK-DOGI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			banking applications based on 'MyPallete' do not verify X.509 certificates from servers, and also do not properly validate certificates with host-mismatch, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2020-5523**		030220/60
hokugin					
hokuriku_bank_portal					
Improper Certificate Validation	28-01-2020	5.8	Android App 'MyPallete' and some of the Android banking applications based on 'MyPallete' do not verify X.509 certificates from servers, and also do not properly validate certificates with host-mismatch, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2020-5523**	N/A	A-HOK-HOKU-030220/61
IBM					
chatbot_with_ibm_watson					
Improper Neutralization of Input During Web Page Generation ('Cross-site	21-01-2020	4.3	The conversation-watson plugin before 0.8.21 for WordPress has a DOM-based XSS vulnerability that is executed when a chat message containing	N/A	A-IBM-CHAT-030220/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			JavaScript is sent. **CVE ID : CVE-2020-7239**		
intelliantech					
aptus_web					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-01-2020	10	Intellian Aptus Web 1.24 allows remote attackers to execute arbitrary OS commands via the Q field within JSON data to the cgi-bin/libagent.cgi URI. NOTE: a valid sid cookie for a login to the intellian default account might be needed. **CVE ID : CVE-2020-7980**	N/A	A-INT-APTU-030220/63
Use of Hard-coded Credentials	27-01-2020	10	Intellian Aptus Web 1.24 has a hardcoded password of 12345678 for the intellian account. **CVE ID : CVE-2020-8000**	N/A	A-INT-APTU-030220/64
aptus					
Use of Hard-coded Credentials	27-01-2020	7.5	The Intellian Aptus application 1.0.2 for Android has hardcoded values for DOWNLOAD_API_KEY and FILE_DOWNLOAD_API_KEY. **CVE ID : CVE-2020-7999**	N/A	A-INT-APTU-030220/65
Use of Hard-coded Credentials	27-01-2020	10	The Intellian Aptus application 1.0.2 for Android has a hardcoded password of intellian for the masteruser FTP account. **CVE ID : CVE-2020-8001**	N/A	A-INT-APTU-030220/66
Jenkins					
websphere_deployer					
Improper	29-01-2020	6.5	Jenkins WebSphere	https://jenki	A-JEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of XML External Entity Reference ('XXE')			Deployer Plugin 1.6.1 and earlier does not configure the XML parser to prevent XXE attacks which can be exploited by a user with Job/Configure permissions. **CVE ID : CVE-2020-2108**	ns.io/security/advisory/2020-01-29/#SECURITY-1719	WEBS-030220/67
jenkins					
Use of Insufficiently Random Values	29-01-2020	7.5	Jenkins 2.213 and earlier, LTS 2.204.1 and earlier improperly reuses encryption key parameters in the Inbound TCP Agent Protocol/3, allowing unauthorized attackers with knowledge of agent names to obtain the connection secrets for those agents, which can be used to connect to Jenkins, impersonating those agents. **CVE ID : CVE-2020-2099**	https://jenkins.io/security/advisory/2020-01-29/#SECURITY-1682	A-JEN-JENK-030220/68
N/A	29-01-2020	5	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier was vulnerable to a UDP amplification reflection denial of service attack on port 33848. **CVE ID : CVE-2020-2100**	https://jenkins.io/security/advisory/2020-01-29/#SECURITY-1641	A-JEN-JENK-030220/69
Information Exposure Through Discrepancy	29-01-2020	3.5	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier did not use a constant-time comparison function for validating connection secrets, which could potentially allow an attacker to use a timing attack to obtain this secret.	https://jenkins.io/security/advisory/2020-01-29/#SECURITY-1659	A-JEN-JENK-030220/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-2101		
Information Exposure Through Discrepancy	29-01-2020	3.5	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier used a non-constant time comparison function when validating an HMAC. **CVE ID : CVE-2020-2102**	https://jenkins.io/security/advisory/2020-01-29/#SECURITY-1660	A-JEN-JENK-030220/71
Information Exposure	29-01-2020	4	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier exposed session identifiers on a user's detail object in the whoAmI diagnostic page. **CVE ID : CVE-2020-2103**	https://jenkins.io/security/advisory/2020-01-29/#SECURITY-1695	A-JEN-JENK-030220/72
Incorrect Authorization	29-01-2020	4	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier allowed users with Overall/Read access to view a JVM memory usage chart. **CVE ID : CVE-2020-2104**	https://jenkins.io/security/advisory/2020-01-29/#SECURITY-1650	A-JEN-JENK-030220/73
Improper Restriction of Rendered UI Layers or Frames	29-01-2020	4.3	REST API endpoints in Jenkins 2.218 and earlier, LTS 2.204.1 and earlier were vulnerable to clickjacking attacks. **CVE ID : CVE-2020-2105**	https://jenkins.io/security/advisory/2020-01-29/#SECURITY-1704	A-JEN-JENK-030220/74
code_coverage_api					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-01-2020	3.5	Jenkins Code Coverage API Plugin 1.1.2 and earlier does not escape the filename of the coverage report used in its view, resulting in a stored XSS vulnerability exploitable by users able to change job configurations. **CVE ID : CVE-2020-2106**	https://jenkins.io/security/advisory/2020-01-29/#SECURITY-1680	A-JEN-CODE-030220/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fortify					
Insufficiently Protected Credentials	29-01-2020	4	Jenkins Fortify Plugin 19.1.29 and earlier stores proxy server passwords unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2020-2107**	https://jenkins.io/security/advisory/2020-01-29/#SECURITY-1565	A-JEN-FORT-030220/76
Jetbrains					
youtrack					
Exposure of Resource to Wrong Sphere	30-01-2020	5	In JetBrains YouTrack before 2019.2.59309, SMTP/Jabber settings could be accessed using backups. **CVE ID : CVE-2020-7912**	https://blog.jetbrains.com/blog/2020/01/24/jetbrains-security-bulletin-q4-2019/	A-JET-YOUT-030220/77
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-01-2020	4.3	JetBrains YouTrack 2019.2 before 2019.2.59309 was vulnerable to XSS via an issue description. **CVE ID : CVE-2020-7913**	https://blog.jetbrains.com/blog/2020/01/24/jetbrains-security-bulletin-q4-2019/	A-JET-YOUT-030220/78
rider					
Improper Verification of Cryptographic Signature	30-01-2020	5	In JetBrains Rider versions 2019.3 EAP2 through 2019.3 EAP7, there were unsigned binaries provided by the Windows installer. This issue was fixed in release version 2019.3. **CVE ID : CVE-2020-7906**	N/A	A-JET-RIDE-030220/79

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
intellij_idea					
Improper Certificate Validation	30-01-2020	5.8	In JetBrains IntelliJ IDEA before 2019.3, some Maven repositories were accessed via HTTP instead of HTTPS. **CVE ID : CVE-2020-7904**	https://blog.jetbrains.com/blog/2020/01/24/jetbrains-security-bulletin-q4-2019/	A-JET-INTE-030220/80
Information Exposure	30-01-2020	5	Ports listened to by JetBrains IntelliJ IDEA before 2019.3 were exposed to the network. **CVE ID : CVE-2020-7905**	https://blog.jetbrains.com/blog/2020/01/24/jetbrains-security-bulletin-q4-2019/	A-JET-INTE-030220/81
teamcity					
Insufficiently Protected Credentials	30-01-2020	4.3	In JetBrains TeamCity before 2019.1.5, reverse tabnabbing was possible on several pages. **CVE ID : CVE-2020-7908**	https://blog.jetbrains.com/blog/2020/01/24/jetbrains-security-bulletin-q4-2019/	A-JET-TEAM-030220/82
Insufficiently Protected Credentials	30-01-2020	5	In JetBrains TeamCity before 2019.1.5, some server-stored passwords could be shown via the web UI. **CVE ID : CVE-2020-7909**	https://blog.jetbrains.com/blog/2020/01/24/jetbrains-security-bulletin-q4-2019/	A-JET-TEAM-030220/83
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-01-2020	3.5	JetBrains TeamCity before 2019.2 was vulnerable to a stored XSS attack by a user with the developer role. **CVE ID : CVE-2020-7910**	https://blog.jetbrains.com/blog/2020/01/24/jetbrains-security-bulletin-q4-2019/	A-JET-TEAM-030220/84
Improper	30-01-2020	4.3	In JetBrains TeamCity	https://blog.j	A-JET-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			before 2019.2, several user-level pages were vulnerable to XSS. **CVE ID : CVE-2020-7911**	etbrains.com/blog/2020/01/24/jetbrains-security-bulletin-q4-2019/	TEAM-030220/85
Jfrog					
artifactory					
N/A	23-01-2020	6.5	In JFrog Artifactory 5.x and 6.x, insecure FreeMarker template processing leads to remote code execution, e.g., by modifying a .ssh/authorized_keys file. Patches are available for various versions between 5.11.8 and 6.16.0. The issue exists because use of the DefaultObjectWrapper class makes certain Java functions accessible to a template. **CVE ID : CVE-2020-7931**	N/A	A-JFR-ARTI-030220/86
Kibokolabs					
chained_quiz					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-01-2020	4.3	The chained-quiz plugin 1.1.8.1 for WordPress has reflected XSS via the wp-admin/admin-ajax.php total_questions parameter. **CVE ID : CVE-2020-7104**	N/A	A-KIB-CHAI-030220/87
learndash					
learndash					
Improper Neutralizatio	16-01-2020	4.3	The LearnDash LMS plugin before 3.1.2 for WordPress	N/A	A-LEA-LEAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			allows XSS via the ld-profile search field. **CVE ID : CVE-2020-7108**		030220/88
libslirp_project					
libslirp					
Out-of-bounds Write	16-01-2020	7.5	tcp_emu in tcp_subr.c in libslirp 4.1.0, as used in QEMU 4.2.0, mismanages memory, as demonstrated by IRC DCC commands in EMU_IRC. This can cause a heap-based buffer overflow or other out-of-bounds access which can lead to a DoS or potential execute arbitrary code. **CVE ID : CVE-2020-7039**	http://www.openwall.com/lists/oss-security/2020/01/16/2	A-LIB-LIBS-030220/89
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-01-2020	5	tftp.c in libslirp 4.1.0, as used in QEMU 4.2.0, does not prevent ..\ directory traversal on Windows. **CVE ID : CVE-2020-7211**	http://www.openwall.com/lists/oss-security/2020/01/17/2	A-LIB-LIBS-030220/90
Magento					
magento					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-01-2020	4.3	Magento versions 2.3.3 and earlier, 2.2.10 and earlier, 1.14.4.3 and earlier, and 1.9.4.3 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information	https://helpx.adobe.com/security/products/magento/apsb20-02.html	A-MAG-MAGE-030220/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure. **CVE ID : CVE-2020-3715**		
Deserialization of Untrusted Data	29-01-2020	10	Magento versions 2.3.3 and earlier, 2.2.10 and earlier, 1.14.4.3 and earlier, and 1.9.4.3 and earlier have a deserialization of untrusted data vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3716**	https://helpx.adobe.com/security/products/magento/apsb20-02.html	A-MAG-MAGE-030220/92
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-01-2020	5	Magento versions 2.3.3 and earlier, 2.2.10 and earlier, 1.14.4.3 and earlier, and 1.9.4.3 and earlier have a path traversal vulnerability. Successful exploitation could lead to sensitive information disclosure. **CVE ID : CVE-2020-3717**	https://helpx.adobe.com/security/products/magento/apsb20-02.html	A-MAG-MAGE-030220/93
N/A	29-01-2020	10	Magento versions 2.3.3 and earlier, 2.2.10 and earlier, 1.14.4.3 and earlier, and 1.9.4.3 and earlier have a security bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3718**	https://helpx.adobe.com/security/products/magento/apsb20-02.html	A-MAG-MAGE-030220/94
Improper Neutralization of Special Elements used in an SQL Command ('SQL	29-01-2020	7.8	Magento versions 2.3.3 and earlier, 2.2.10 and earlier, 1.14.4.3 and earlier, and 1.9.4.3 and earlier have an sql injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	https://helpx.adobe.com/security/products/magento/apsb20-02.html	A-MAG-MAGE-030220/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			**CVE ID : CVE-2020-3719**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-01-2020	4.3	Magento versions 2.3.3 and earlier, 2.2.10 and earlier, 1.14.4.3 and earlier, and 1.9.4.3 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure. **CVE ID : CVE-2020-3758**	https://helpx.adobe.com/security/products/magento/apsb20-02.html	A-MAG-MAGE-030220/96
mirumee					
saleor					
Information Exposure	24-01-2020	5	An issue was discovered in Mirumee Saleor 2.x before 2.9.1. Incorrect access control in the checkoutCustomerAttach mutations allows attackers to attach their checkouts to any user ID and consequently leak user data (e.g., name, address, and previous orders of any other customer). **CVE ID : CVE-2020-7964**	N/A	A-MIR-SALE-030220/97
Mozilla					
firefox					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-01-2020	4.3	A XSS vulnerability was found in Apache NiFi 1.0.0 to 1.10.0. Malicious scripts could be injected to the UI through action by an unaware authenticated user in Firefox. Did not appear to occur in other browsers. **CVE ID : CVE-2020-1933**	https://nifi.apache.org/security.html#CVE-2020-1933	A-MOZ-FIRE-030220/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
naganobank					
nagagin					
Improper Certificate Validation	28-01-2020	5.8	Android App 'MyPallete' and some of the Android banking applications based on 'MyPallete' do not verify X.509 certificates from servers, and also do not properly validate certificates with host-mismatch, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2020-5523**	N/A	A-NAG-NAGA-030220/99
netty					
netty					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	27-01-2020	5	Netty 4.1.43.Final allows HTTP Request Smuggling because it mishandles Transfer-Encoding whitespace (such as a [space]Transfer-Encoding:chunked line) and a later Content-Length header. This issue exists because of an incomplete fix for CVE-2019-16869. **CVE ID : CVE-2020-7238**	N/A	A-NET-NETT-030220/100
Nttdata					
mypallete					
Improper Certificate Validation	28-01-2020	5.8	Android App 'MyPallete' and some of the Android banking applications based on 'MyPallete' do not verify X.509 certificates from	N/A	A-NTT-MYPA-030220/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			servers, and also do not properly validate certificates with host-mismatch, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2020-5523**		
Openbsd					
opensmtpd					
Unchecked Return Value	29-01-2020	10	smtp_mailaddr in smtp_session.c in OpenSMTPD 6.6, as used in OpenBSD 6.6 and other products, allows remote attackers to execute arbitrary commands as root via a crafted SMTP session, as demonstrated by shell metacharacters in a MAIL FROM field. This affects the "uncommented" default configuration. The issue exists because of an incorrect return value upon failure of input validation. **CVE ID : CVE-2020-7247**	https://github.com/openbsd/src/commit/9dcfda045474d8903224d175907bfc29761dcb45, https://www.openbsd.org/security.html	A-OPE-OPEN-030220/102
Ossec					
ossec					
Out-of-bounds Write	30-01-2020	6.5	In OSSEC-HIDS 2.7 through 3.5.0, the server component responsible for log analysis (ossec-analysisd) is vulnerable to a heap-based buffer overflow in the rootcheck decoder component via an	N/A	A-OSS-OSSE-030220/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated client. **CVE ID : CVE-2020-8442**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-01-2020	2.1	In OSSEC-HIDS 2.7 through 3.5.0, the server component responsible for log analysis (ossec-analysisd) is vulnerable to path traversal (with write access) via crafted syscheck messages written directly to the analysisd UNIX domain socket by a local user. **CVE ID : CVE-2020-8446**	N/A	A-OSS-OSSE-030220/104
NULL Pointer Dereference	30-01-2020	2.1	In OSSEC-HIDS 2.7 through 3.5.0, the server component responsible for log analysis (ossec-analysisd) is vulnerable to a denial of service (NULL pointer dereference) via crafted messages written directly to the analysisd UNIX domain socket by a local user. **CVE ID : CVE-2020-8448**	N/A	A-OSS-OSSE-030220/105
Parallels					
parallels					
Cleartext Storage of Sensitive Information	21-01-2020	7.6	Parallels 13 uses cleartext HTTP as part of the update process, allowing man-in-the-middle attacks. Users of out-of-date versions are presented with a pop-up window for a parallels_updates.xml file on the http://update.parallels.com web site. **CVE ID : CVE-2020-7213**	N/A	A-PAR-PARA-030220/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
peerigon					
angular-expressions					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-01-2020	6.8	Angular Expressions before version 1.0.1 has a remote code execution vulnerability if you call expressions.compile(userControlledInput) where userControlledInput is text that comes from user input. If running angular-expressions in the browser, an attacker could run any browser script when the application code calls expressions.compile(userControlledInput). If running angular-expressions on the server, an attacker could run any Javascript expression, thus gaining Remote Code Execution. **CVE ID : CVE-2020-5219**	https://github.com/peerigon/angular-expressions/security/advisories/GHSA-hxhm-96pp-2m43	A-PEE-ANGU-030220/107
pivotal_software					
spring_framework					
Cross-Site Request Forgery (CSRF)	17-01-2020	2.6	Spring Framework, versions 5.2.x prior to 5.2.3 are vulnerable to CSRF attacks through CORS preflight requests that target Spring MVC (spring-webmvc module) or Spring WebFlux (spring-webflux module) endpoints. Only non-authenticated endpoints are vulnerable because preflight requests should not include credentials and therefore requests should	https://pivotal.io/security/cve-2020-5397	A-PIV-SPRI-030220/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fail authentication. However a notable exception to this are Chrome based browsers when using client certificates for authentication since Chrome sends TLS client certificates in CORS preflight requests in violation of spec requirements. No HTTP body can be sent or received as a result of this attack. **CVE ID : CVE-2020-5397**		
Download of Code Without Integrity Check	17-01-2020	7.6	In Spring Framework, versions 5.2.x prior to 5.2.3, versions 5.1.x prior to 5.1.13, and versions 5.0.x prior to 5.0.16, an application is vulnerable to a reflected file download (RFD) attack when it sets a "Content-Disposition" header in the response where the filename attribute is derived from user supplied input. **CVE ID : CVE-2020-5398**	https://pivotal.io/security/cve-2020-5398	A-PIV-SPRI-030220/109
Plone					
plone					
URL Redirection to Untrusted Site ('Open Redirect')	23-01-2020	5.8	An open redirect on the login form (and possibly other places) in Plone 4.0 through 5.2.1 allows an attacker to craft a link to a Plone Site that, when followed, and possibly after	N/A	A-PLO-PLON-030220/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			login, will redirect to an attacker's site. **CVE ID : CVE-2020-7936**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-01-2020	3.5	An XSS issue in the title field in Plone 5.0 through 5.2.1 allows users with a certain privilege level to insert JavaScript that will be executed when other users access the site. **CVE ID : CVE-2020-7937**	N/A	A-PLO-PLON-030220/111
Improper Privilege Management	23-01-2020	6.5	plone.restapi in Plone 5.2.0 through 5.2.1 allows users with a certain privilege level to escalate their privileges up to the highest level. **CVE ID : CVE-2020-7938**	N/A	A-PLO-PLON-030220/112
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-01-2020	6.5	SQL Injection in DTML or in connection objects in Plone 4.0 through 5.2.1 allows users to perform unwanted SQL queries. (This is a problem in Zope.) **CVE ID : CVE-2020-7939**	N/A	A-PLO-PLON-030220/113
Weak Password Requirements	23-01-2020	5	Missing password strength checks on some forms in Plone 4.3 through 5.2.0 allow users to set weak passwords, leading to easier cracking. **CVE ID : CVE-2020-7940**	N/A	A-PLO-PLON-030220/114
Improper Privilege Management	23-01-2020	7.5	A privilege escalation issue in plone.app.contenttypes in Plone 4.3 through 5.2.1 allows users to PUT	N/A	A-PLO-PLON-030220/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(overwrite) some content without needing write permission. **CVE ID : CVE-2020-7941**		
privatebin					
privatebin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-01-2020	2.1	In PrivateBin versions 1.2.0 before 1.2.2, and 1.3.0 before 1.3.2, a persistent XSS attack is possible. Under certain conditions, a user provided attachment file name can inject HTML leading to a persistent Cross-site scripting (XSS) vulnerability. The vulnerability has been fixed in PrivateBin v1.3.2 & v1.2.2. Admins are urged to upgrade to these versions to protect the affected users. **CVE ID : CVE-2020-5223**	https://github.com/PrivateBin/PrivateBin/security/advisories/GHSA-8j72-p2wm-6738	A-PRI-PRIV-030220/116
Python					
python					
Improper Input Validation	28-01-2020	4.3	In Python (CPython) 3.6 through 3.6.10, 3.7 through 3.7.6, and 3.8 through 3.8.1, an insecure dependency load upon launch on Windows 7 may result in an attacker's copy of api-ms-win-core-path-l1-1-0.dll being loaded and used instead of the system's copy. Windows 8 and later are unaffected. **CVE ID : CVE-2020-8315**	N/A	A-PYT-PYTH-030220/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Qdpm					
qdpm					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-01-2020	6.5	A remote code execution (RCE) vulnerability exists in qdPM 9.1 and earlier. An attacker can upload a malicious PHP code file via the profile photo functionality, by leveraging a path traversal vulnerability in the users['photop_preview'] delete photo feature, allowing bypass of .htaccess protection. NOTE: this issue exists because of an incomplete fix for CVE-2015-3884. **CVE ID : CVE-2020-7246**	N/A	A-QDP-QDPM-030220/118
Qemu					
qemu					
Out-of-bounds Write	16-01-2020	7.5	tcp_emu in tcp_subr.c in libslirp 4.1.0, as used in QEMU 4.2.0, mismanages memory, as demonstrated by IRC DCC commands in EMU_IRC. This can cause a heap-based buffer overflow or other out-of-bounds access which can lead to a DoS or potential execute arbitrary code. **CVE ID : CVE-2020-7039**	http://www.openwall.com/lists/oss-security/2020/01/16/2	A-QEM-QEMU-030220/119
Improper Limitation of a Pathname to a Restricted Directory	21-01-2020	5	tftp.c in libslirp 4.1.0, as used in QEMU 4.2.0, does not prevent ..\ directory traversal on Windows. **CVE ID : CVE-2020-7211**	http://www.openwall.com/lists/oss-security/2020/01/17/2	A-QEM-QEMU-030220/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')					
redislabs					
hiredis					
NULL Pointer Dereference	16-01-2020	5	async.c and dict.c in libhiredis.a in hiredis through 0.14.0 allow a NULL pointer dereference because malloc return values are unchecked. **CVE ID : CVE-2020-7105**	N/A	A-RED-HIRE-030220/121
rubygeocoder					
geocoder					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-01-2020	7.5	sql.rb in Geocoder before 1.6.1 allows Boolean-based SQL injection when within_bounding_box is used in conjunction with untrusted sw_lat, sw_lng, ne_lat, or ne_lng data. **CVE ID : CVE-2020-7981**	N/A	A-RUB-GEOC-030220/122
shikokubank					
shikoku_bank					
Improper Certificate Validation	28-01-2020	5.8	Android App 'MyPallete' and some of the Android banking applications based on 'MyPallete' do not verify X.509 certificates from servers, and also do not properly validate certificates with host-mismatch, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	N/A	A-SHI-SHIK-030220/123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5523		
sihd-bk					
ikeda_senshu_bank					
Improper Certificate Validation	28-01-2020	5.8	Android App 'MyPallete' and some of the Android banking applications based on 'MyPallete' do not verify X.509 certificates from servers, and also do not properly validate certificates with host-mismatch, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2020-5523**	N/A	A-SIH-IKED-030220/124
simplejobscript					
simplejobscript					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-01-2020	7.5	An issue was discovered in Simplejobscript.com SJS before 1.65. There is unauthenticated SQL injection via the search engine. The parameter is landing_location. The function is countSearchedJobs(). The file is _lib/class.Job.php. **CVE ID : CVE-2020-7229**	N/A	A-SIM-SIMP-030220/125
Simplesamlphp					
simplesamlphp					
Information Exposure Through Log Files	24-01-2020	5.5	Log injection in SimpleSAMLphp before version 1.18.4. The www/erroreport.php script, which receives error	https://github.com/simplesamlphp/simplesamlphp/security/advis	A-SIM-SIMP-030220/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reports and sends them via email to the system administrator, did not properly sanitize the report identifier obtained from the request. This allows an attacker, under specific circumstances, to inject new log lines by manually crafting this report ID. When configured to use the file logging handler, SimpleSAMLphp will output all its logs by appending each log line to a given file. Since the reportID parameter received in a request sent to www/errorreport.php was not properly sanitized, it was possible to inject newline characters into it, effectively allowing a malicious user to inject new log lines with arbitrary content. **CVE ID : CVE-2020-5225**	ories/GHSA-6gc6-m364-85ww	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-01-2020	3.5	Cross-site scripting in SimpleSAMLphp before version 1.18.4. The www/erroreport.php script allows error reports to be submitted and sent to the system administrator. Starting with SimpleSAMLphp 1.18.0, a new SimpleSAML\Utils\EMail class was introduced to handle sending emails, implemented as a wrapper	https://github.com/simplesamlphp/simplesamlphp/security/advisories/GHSA-mj9p-v2r8-wf8w	A-SIM-SIMP-030220/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of an external dependency. This new wrapper allows us to use Twig templates in order to create the email sent with an error report. Since Twig provides automatic escaping of variables, manual escaping of the free-text field in www/errorreport.php was removed to avoid double escaping. However, for those not using the new user interface yet, an email template is hardcoded into the class itself in plain PHP. Since no escaping is provided in this template, it is then possible to inject HTML inside the template by manually crafting the contents of the free-text field. **CVE ID : CVE-2020-5226**		
tohoku-bank					
tougin					
Improper Certificate Validation	28-01-2020	5.8	Android App 'MyPallete' and some of the Android banking applications based on 'MyPallete' do not verify X.509 certificates from servers, and also do not properly validate certificates with host-mismatch, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	N/A	A-TOH-TOUG-030220/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5523		
Troglobit					
uftpd					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-01-2020	6.4	In uftpd before 2.11, it is possible for an unauthenticated user to perform a directory traversal attack using multiple different FTP commands and read and write to arbitrary locations on the filesystem due to the lack of a well-written chroot jail in compose_abspath(). This has been fixed in version 2.11 **CVE ID : CVE-2020-5221**	https://github.com/troglobit/uftpd/security/advisories/GHSA-wmx8-v7mx-6x9h	A-TRO-UFTP-030220/129
Twitter					
secure_headers					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-01-2020	4	In Secure Headers (RubyGem secure_headers), a directive injection vulnerability is present in versions before 3.9.0, 5.2.0, and 6.3.0. If user-supplied input was passed into append/override_content_security_policy_directives, a newline could be injected leading to limited header injection. Upon seeing a newline in the header, rails will silently create a new Content-Security-Policy header with the remaining value of the original string. It will continue to create new headers for each newline. This has been fixed	https://github.com/twitter/secure_headers/security/advisories/GHSA-w978-rmpf-qmwg	A-TWI-SECU-030220/130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in 6.3.0, 5.2.0, and 3.9.0. **CVE ID : CVE-2020-5216**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-01-2020	4.3	In Secure Headers (RubyGem secure_headers), a directive injection vulnerability is present in versions before 3.8.0, 5.1.0, and 6.2.0. If user-supplied input was passed into append/override_content_security_policy_directives, a semicolon could be injected leading to directive injection. This could be used to e.g. override a script-src directive. Duplicate directives are ignored and the first one wins. The directives in secure_headers are sorted alphabetically so they pretty much all come before script-src. A previously undefined directive would receive a value even if SecureHeaders::OPT_OUT was supplied. The fixed versions will silently convert the semicolons to spaces and emit a deprecation warning when this happens. This will result in innocuous browser console messages if being exploited/accidentally used. In future releases, we will raise application errors resulting in 500s. Depending on what major version you are using, the fixed versions are 6.2.0,	https://github.com/twitter/secure_headers/security/advisories/GHSA-xq52-rv6w-397c	A-TWI-SECU-030220/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.1.0, 3.8.0. **CVE ID : CVE-2020-5217**		
Typo3					
typo3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-01-2020	4.3	svg.swf in TYPO3 6.2.0 to 6.2.38 ELTS and 7.0.0 to 7.1.0 could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack on a targeted system. This may be at a contrib/websvg/svg.swf pathname. **CVE ID : CVE-2020-8091**	N/A	A-TYP-TYPO-030220/132
Valvesoftware					
dota_2					
N/A	27-01-2020	6.8	schemasystem.dll in Valve Dota 2 before 7.23f allows remote attackers to achieve code execution or denial of service by creating a gaming server and inviting a victim to this server, because a crafted map is mishandled during a GetValue call. **CVE ID : CVE-2020-7949**	N/A	A-VAL-DOTA-030220/133
N/A	27-01-2020	6.8	meshsystem.dll in Valve Dota 2 before 7.23f allows remote attackers to achieve code execution or denial of service by creating a gaming server and inviting a victim to this server, because a crafted map is mishandled during a vulnerable function call.	N/A	A-VAL-DOTA-030220/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7950		
N/A	27-01-2020	6.8	meshsystem.dll in Valve Dota 2 before 7.23e allows remote attackers to achieve code execution or denial of service by creating a gaming server and inviting a victim to this server, because a crafted map is affected by memory corruption. **CVE ID : CVE-2020-7951**	N/A	A-VAL-DOTA-030220/135
N/A	27-01-2020	6.8	rendersystemdx9.dll in Valve Dota 2 before 7.23f allows remote attackers to achieve code execution or denial of service by creating a gaming server and inviting a victim to this server, because a crafted map is affected by memory corruption. **CVE ID : CVE-2020-7952**	N/A	A-VAL-DOTA-030220/136
virglrenderer_project					
virglrenderer					
NULL Pointer Dereference	27-01-2020	2.1	A NULL pointer dereference in vrend_renderer.c in virglrenderer through 0.8.1 allows attackers to cause a denial of service via commands that attempt to launch a grid without previously providing a Compute Shader (CS). **CVE ID : CVE-2020-8002**	N/A	A-VIR-VIRG-030220/137
Double Free	27-01-2020	2.1	A double-free vulnerability in vrend_renderer.c in virglrenderer through 0.8.1	N/A	A-VIR-VIRG-030220/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to cause a denial of service by triggering texture allocation failure, because vrend_renderer_resource_allocated_texture is not an appropriate place for a free. **CVE ID : CVE-2020-8003**		
Vmware					
workspace_one_boxer					
Improper Certificate Validation	17-01-2020	4.3	VMware Workspace ONE SDK and dependent mobile application updates address sensitive information disclosure vulnerability. **CVE ID : CVE-2020-3940**	https://www.vmware.com/security/advisories/VMSA-2020-0001.html	A-VMW-WORK-030220/139
workspace_one_content					
Improper Certificate Validation	17-01-2020	4.3	VMware Workspace ONE SDK and dependent mobile application updates address sensitive information disclosure vulnerability. **CVE ID : CVE-2020-3940**	https://www.vmware.com/security/advisories/VMSA-2020-0001.html	A-VMW-WORK-030220/140
workspace_one_intelligent_hub					
Improper Certificate Validation	17-01-2020	4.3	VMware Workspace ONE SDK and dependent mobile application updates address sensitive information disclosure vulnerability. **CVE ID : CVE-2020-3940**	https://www.vmware.com/security/advisories/VMSA-2020-0001.html	A-VMW-WORK-030220/141
workspace_one_notebook					
Improper Certificate Validation	17-01-2020	4.3	VMware Workspace ONE SDK and dependent mobile application updates address sensitive information disclosure vulnerability.	https://www.vmware.com/security/advisories/VMSA-2020-0001.html	A-VMW-WORK-030220/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3940		
workspace_one_people					
Improper Certificate Validation	17-01-2020	4.3	VMware Workspace ONE SDK and dependent mobile application updates address sensitive information disclosure vulnerability. **CVE ID : CVE-2020-3940**	https://www.vmware.com/security/advisories/VMSA-2020-0001.html	A-VMW-WORK-030220/143
workspace_one_piv-d_manager					
Improper Certificate Validation	17-01-2020	4.3	VMware Workspace ONE SDK and dependent mobile application updates address sensitive information disclosure vulnerability. **CVE ID : CVE-2020-3940**	https://www.vmware.com/security/advisories/VMSA-2020-0001.html	A-VMW-WORK-030220/144
workspace_one_sdk					
Improper Certificate Validation	17-01-2020	4.3	VMware Workspace ONE SDK and dependent mobile application updates address sensitive information disclosure vulnerability. **CVE ID : CVE-2020-3940**	https://www.vmware.com/security/advisories/VMSA-2020-0001.html	A-VMW-WORK-030220/145
workspace_one_sdk_\(objective-c\)					
Improper Certificate Validation	17-01-2020	4.3	VMware Workspace ONE SDK and dependent mobile application updates address sensitive information disclosure vulnerability. **CVE ID : CVE-2020-3940**	https://www.vmware.com/security/advisories/VMSA-2020-0001.html	A-VMW-WORK-030220/146
workspace_one_web					
Improper Certificate Validation	17-01-2020	4.3	VMware Workspace ONE SDK and dependent mobile application updates address sensitive information disclosure vulnerability. **CVE ID : CVE-2020-3940**	https://www.vmware.com/security/advisories/VMSA-2020-0001.html	A-VMW-WORK-030220/147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
webfactoryltd					
wp_database_reset					
Improper Privilege Management	16-01-2020	6.5	The WordPress plugin, WP Database Reset through 3.1, contains a flaw that gave any authenticated user, with minimal permissions, the ability (with a simple wp-admin/admin.php?db-reset-tables[]=users request) to escalate their privileges to administrator while dropping all other users from the table. **CVE ID : CVE-2020-7047**	N/A	A-WEB-WP_D-030220/148
Improper Privilege Management	16-01-2020	6.4	The WordPress plugin, WP Database Reset through 3.1, contains a flaw that allowed any unauthenticated user to reset any table in the database to the initial WordPress set-up state (deleting all site content stored in that table), as demonstrated by a wp-admin/admin-post.php?db-reset-tables[]=comments URI. **CVE ID : CVE-2020-7048**	N/A	A-WEB-WP_D-030220/149
Wireshark					
wireshark					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	16-01-2020	5	In Wireshark 3.2.x before 3.2.1, the WASSP dissector could crash. This was addressed in epan/dissectors/packet-wassp.c by using >= and <= to resolve off-by-one errors.	N/A	A-WIR-WIRE-030220/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			**CVE ID : CVE-2020-7044**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-01-2020	5	In Wireshark 3.0.x before 3.0.8, the BT ATT dissector could crash. This was addressed in epan/dissectors/packet-btatt.c by validating opcodes. **CVE ID : CVE-2020-7045**	N/A	A-WIR-WIRE-030220/151
wpseeds					
wp_database_backup					
Files or Directories Accessible to External Parties	20-01-2020	5	The WP Database Backup plugin through 5.5 for WordPress stores downloads by default locally in the directory wp-content/uploads/db-backup/. This might allow attackers to read ZIP archives by guessing random ID numbers, guessing date strings with a 2020_{0..1}{0..2}_{0..3}{0..9} format, guessing UNIX timestamps, and making HTTPS requests with the complete guessed URL. **CVE ID : CVE-2020-7241**	N/A	A-WPS-WP_D-030220/152
Xmlsoft					
libxml2					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-01-2020	5	xmlStringLenDecodeEntities in parser.c in libxml2 2.9.10 has an infinite loop in a certain end-of-file situation. **CVE ID : CVE-2020-7595**	N/A	A-XML-LIBX-030220/153
Zohocorp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
manageengine_servicedesk_plus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-01-2020	3.5	Zoho ManageEngine ServiceDesk Plus 11.0 Build 11007 allows XSS. This issue was fixed in version 11.0 Build 11010, SD-83959. **CVE ID : CVE-2020-6843**	https://www.manageengine.com/products/service-desk/readme.html#11010%20-%20SD-83959	A-ZOH-MANA-030220/154
Operating System					
a1					
wlan_box_adb_vv2220_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-01-2020	3.5	The Username field in the Storage Service settings of A1 WLAN Box ADB VV2220v2 devices allows stored XSS (after a successful Administrator login). **CVE ID : CVE-2020-8090**	N/A	O-A1-WLAN-030220/155
Arris					
ruckus_zoneflex_r500_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-01-2020	9	Ruckus ZoneFlex R500 104.0.0.0.1347 devices allow an authenticated attacker to execute arbitrary OS commands via the hidden /forms/nslookupHandler form, as demonstrated by the nslookuptarget=|cat${IFS} substring. **CVE ID : CVE-2020-8438**	N/A	O-ARR-RUCK-030220/156
Asus					
rt-ac66u_firmware					
Improper	28-01-2020	4.3	ASUS WRT-AC66U 3 RT	N/A	O-ASU-RT-A-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			3.0.0.4.372_67 devices allow XSS via the Client Name field to the Parental Control feature. **CVE ID : CVE-2020-7997**		030220/157
Cisco					
sf302-08pp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SF30-030220/158
sf302-08mpp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on	N/A	O-CIS-SF30-030220/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf300-24_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18	N/A	O-CIS-SF30-030220/160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3147		
sf300-24p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SF30-030220/161
sf300-24mp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an	N/A	O-CIS-SF30-030220/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf300-24pp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SF30-030220/163
sf300-48_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of	N/A	O-CIS-SF30-030220/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf300-48p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases	N/A	O-CIS-SF30-030220/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf300-48pp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SF30-030220/166
sf500-24_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by	N/A	O-CIS-SF50-030220/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf500-24p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SF50-030220/168
sf500-48_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an	N/A	O-CIS-SF50-030220/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf500-48p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS	N/A	O-CIS-SF50-030220/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg500-28_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG50-030220/171
sg500-28p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web	N/A	O-CIS-SG50-030220/172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg500-28mpp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG50-030220/173
sg500-52_firmware					
Improper	30-01-2020	7.8	A vulnerability in the web	N/A	O-CIS-SG50-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		030220/174
sg500-52p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an	N/A	O-CIS-SG50-030220/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg500-52mp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG50-030220/176
sg500x-24_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to	N/A	O-CIS-SG50-030220/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg500x-48_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG50-030220/178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg500x-48p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG50-030220/179
sg250x-24_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An	N/A	O-CIS-SG25-030220/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250x-24p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based	N/A	O-CIS-SG25-030220/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information. **CVE ID : CVE-2020-3121**		
sg250x-48_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SG25-030220/182
sg250x-48p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct	N/A	O-CIS-SG25-030220/183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-08_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to	N/A	O-CIS-SG25-030220/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-08hp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SG25-030220/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg250-10p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SG25-030220/186
sg250-18_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability	N/A	O-CIS-SG25-030220/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-26_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could	N/A	O-CIS-SG25-030220/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sg250-26hp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SG25-030220/189
sg250-26p_firmware					
Improper Neutralizatio	26-01-2020	4.3	A vulnerability in the web-based management	N/A	O-CIS-SG25-030220/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-50_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based	N/A	O-CIS-SG25-030220/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-50hp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the	N/A	O-CIS-SG25-030220/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sg250-50p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SG25-030220/193
sg250-24_firmware					
Improper Neutralization of Input During Web Page	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could	N/A	O-CIS-SG25-030220/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-24p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this	N/A	O-CIS-SG25-030220/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-48_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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.	N/A	O-CIS-SG25-030220/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3121		
sg250-48hp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SG25-030220/197
sf350-48_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the	N/A	O-CIS-SF35-030220/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sf350-48p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A	N/A	O-CIS-SF35-030220/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sf350-48mp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SF35-030220/200
sg350-10_firmware					
Improper	26-01-2020	4.3	A vulnerability in the web-	N/A	O-CIS-SG35-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		030220/201
sg350-10p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied	N/A	O-CIS-SG35-030220/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg350-10mp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could allow the attacker to execute arbitrary script	N/A	O-CIS-SG35-030220/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sg355-10mp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SG35-030220/204
sg350-28_firmware					
Improper Neutralization of Input During Web	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and	N/A	O-CIS-SG35-030220/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg350-28p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An	N/A	O-CIS-SG35-030220/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg350-28mp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based	N/A	O-CIS-SG35-030220/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information. **CVE ID : CVE-2020-3121**		
sx550x-16ft_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SX55-030220/208
sx550x-24ft_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct	N/A	O-CIS-SX55-030220/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sx550x-12ft_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to	N/A	O-CIS-SX55-030220/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sx550x-24_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SX55-030220/211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sx550x-52_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SX55-030220/212
sg550x-24_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability	N/A	O-CIS-SG55-030220/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg550x-24p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could	N/A	O-CIS-SG55-030220/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sg550x-24mp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SG55-030220/215
sg550x-24mpp_firmware					
Improper Neutralizatio	26-01-2020	4.3	A vulnerability in the web-based management	N/A	O-CIS-SG55-030220/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg550x-48_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based	N/A	O-CIS-SG55-030220/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg550x-48p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the	N/A	O-CIS-SG55-030220/218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sg550x-48mp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SG55-030220/219
sg200-18_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of	N/A	O-CIS-SG20-030220/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-26_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases	N/A	O-CIS-SG20-030220/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-26p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG20-030220/222
sg200-50_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by	N/A	O-CIS-SG20-030220/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-50p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG20-030220/224
sg300-10_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an	N/A	O-CIS-SG30-030220/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-10mp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS	N/A	O-CIS-SG30-030220/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-10mpp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG30-030220/227
sg300-10sfp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web	N/A	O-CIS-SG30-030220/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-10p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG30-030220/229
sg300-10pp_firmware					
Improper	30-01-2020	7.8	A vulnerability in the web	N/A	O-CIS-SG30-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		030220/230
sg300-20_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an	N/A	O-CIS-SG30-030220/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-28_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG30-030220/232
sg300-28p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to	N/A	O-CIS-SG30-030220/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-28pp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG30-030220/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-28mp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG30-030220/235
sg300-52_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful	N/A	O-CIS-SG30-030220/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-52p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG30-030220/237
sg300-52mp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on	N/A	O-CIS-SG30-030220/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf300-08_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18	N/A	O-CIS-SF30-030220/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3147		
sf302-08_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SF30-030220/240
sf302-08mp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an	N/A	O-CIS-SF30-030220/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf302-08p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SF30-030220/242
sf550x-24_firmware					
Improper Neutralization of Input During Web Page	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could	N/A	O-CIS-SF55-030220/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sf550x-24p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this	N/A	O-CIS-SF55-030220/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sf550x-48_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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.	N/A	O-CIS-SF55-030220/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3121		
sf550x-48p_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	O-CIS-SF55-030220/246
sf550x-48mp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the	N/A	O-CIS-SF55-030220/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg200-24_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability	N/A	O-CIS-SG20-030220/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-24p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG20-030220/249
sg200-24fp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could	N/A	O-CIS-SG20-030220/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-48_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG20-030220/251
sg200-48p_firmware					
Improper Input	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business	N/A	O-CIS-SG20-030220/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sd-wan_firmware					
Improper Privilege Management	26-01-2020	7.2	A vulnerability in the CLI of the Cisco SD-WAN Solution vManage software could allow an authenticated, local attacker to elevate privileges to root-level privileges on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted file to the affected system. An exploit could allow the attacker to elevate privileges to root-level privileges. **CVE ID : CVE-2020-3115**	N/A	O-CIS-SD-W-030220/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg200-50fp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG20-030220/254
sg200-26fp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful	N/A	O-CIS-SG20-030220/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-10fp_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG20-030220/256
sg200-08_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on	N/A	O-CIS-SG20-030220/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-08p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18	N/A	O-CIS-SG20-030220/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3147		
sg500xg-8f8t_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	O-CIS-SG50-030220/259
sg500x-24p_firmware					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an	N/A	O-CIS-SG50-030220/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
comtechtel					
stampede_fx-1010_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-01-2020	9	Comtech Stampede FX-1010 7.4.3 devices allow remote authenticated administrators to achieve remote code execution by navigating to the Diagnostics Trace Route page and entering shell metacharacters in the Target IP address field. (In some cases, authentication can be achieved with the comtech password for the comtech account.) **CVE ID : CVE-2020-7242**	N/A	O-COM-STAM-030220/261
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-01-2020	9	Comtech Stampede FX-1010 7.4.3 devices allow remote authenticated administrators to achieve remote code execution by navigating to the Fetch URL page and entering shell metacharacters in the URL field. (In some cases, authentication can be achieved with the comtech password for the comtech account.)	N/A	O-COM-STAM-030220/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7243		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-01-2020	9	Comtech Stampede FX-1010 7.4.3 devices allow remote authenticated administrators to achieve remote code execution by navigating to the Poll Routes page and entering shell metacharacters in the Router IP Address field. (In some cases, authentication can be achieved with the comtech password for the comtech account.) **CVE ID : CVE-2020-7244**	N/A	O-COM-STAM-030220/263
Debian					
debian_linux					
Information Exposure	21-01-2020	2.1	apt-cacher-ng through 3.3 allows local users to obtain sensitive information by hijacking the hardcoded TCP port. The /usr/lib/apt-cacher-ng/acngtool program attempts to connect to apt-cacher-ng via TCP on localhost port 3142, even if the explicit SocketPath=/var/run/apt-cacher-ng/socket command-line option is passed. The cron job /etc/cron.daily/apt-cacher-ng (which is active by default) attempts this periodically. Because 3142 is an unprivileged port, any local user can try to bind to this port and will receive requests from acngtool. There can be sensitive data	N/A	O-DEB-DEBI-030220/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in these requests, e.g., if AdminAuth is enabled in /etc/apt-cacher-ng/security.conf. This sensitive data can leak to unprivileged local users that manage to bind to this port before the apt-cacher-ng daemon can. **CVE ID : CVE-2020-5202**		
Unchecked Return Value	29-01-2020	10	smtp_mailaddr in smtp_session.c in OpenSMTPD 6.6, as used in OpenBSD 6.6 and other products, allows remote attackers to execute arbitrary commands as root via a crafted SMTP session, as demonstrated by shell metacharacters in a MAIL FROM field. This affects the "uncommented" default configuration. The issue exists because of an incorrect return value upon failure of input validation. **CVE ID : CVE-2020-7247**	https://github.com/openbsd/src/commit/9dcfda045474d8903224d175907bfc29761dcb45, https://www.openbsd.org/security.html	O-DEB-DEBI-030220/265
Eaton					
5p_850_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-01-2020	3.5	An issue was discovered on Eaton 5P 850 devices. The Ubicacion SAI field allows XSS attacks by an administrator. **CVE ID : CVE-2020-7915**	N/A	O-EAT-5P_8-030220/266
Huawei					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
honor_v30_firmware					
Improper Authentication	21-01-2020	4.3	Honor V30 smartphones with versions earlier than 10.0.1.135(C00E130R4P1) have an improper authentication vulnerability. Certain applications do not properly validate the identity of another application who would call its interface. An attacker could trick the user into installing a malicious application. Successful exploit could allow unauthorized actions leading to information disclosure. **CVE ID : CVE-2020-1788**	N/A	O-HUA-HONO-030220/267
mate_20_firmware					
Improper Authentication	21-01-2020	3.6	HUAWEI Mate 20 smart phones with versions earlier than 10.0.0.175(C00E70R3P8) have an insufficient authentication vulnerability. A local attacker with high privilege can execute a specific command to exploit this vulnerability. Successful exploitation may cause information leak and compromise the availability of the smart phones.Affected product versions include: HUAWEI Mate 20 versions Versions earlier than	N/A	O-HUA-MATE-030220/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.175(C00E70R3P8) **CVE ID : CVE-2020-1840**		
kmccontrols					
bac-a1616bc_firmware					
Use of Hard-coded Credentials	19-01-2020	10	KMS Controls BAC-A1616BC BACnet devices have a cleartext password of snowman in the BACKDOOR_NAME variable in the BC_Logon.swf file. **CVE ID : CVE-2020-7233**	N/A	O-KMC-BAC--030220/269
Linux					
linux_kernel					
Use After Free	29-01-2020	3.6	fs/namei.c in the Linux kernel before 5.5 has a may_create_in_sticky use-after-free, which allows local users to cause a denial of service (OOPS) or possibly obtain sensitive information from kernel memory, aka CID-d0cb50185ae9. One attack vector may be an open system call for a UNIX domain socket, if the socket is being moved to a new parent directory and its old parent directory is being removed. **CVE ID : CVE-2020-8428**	N/A	O-LIN-LINU-030220/270
meinbergglobal					
lantime_m300_firmware					
Improper Neutralization of Special Elements	20-01-2020	9	Meinberg Lantime M300 and M1000 devices allow attackers (with privileges to configure a device) to	N/A	O-MEI-LANT-030220/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary OS commands by editing the /config/netconf.cmd script (aka Extended Network Configuration). **CVE ID : CVE-2020-7240**		
lantime_m1000_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-01-2020	9	Meinberg Lantime M300 and M1000 devices allow attackers (with privileges to configure a device) to execute arbitrary OS commands by editing the /config/netconf.cmd script (aka Extended Network Configuration). **CVE ID : CVE-2020-7240**	N/A	O-MEI-LANT-030220/272
Microsoft					
windows					
Uncontrolled Resource Consumption	26-01-2020	4	A vulnerability in the Cisco Webex Teams client for Windows could allow an authenticated, remote attacker to cause the client to crash, resulting in a denial of service (DoS) condition. The attacker needs a valid developer account to exploit this vulnerability. The vulnerability is due to insufficient input validation when processing received adaptive cards. The attacker could exploit this vulnerability by sending an adaptive card with malicious content to an existing user of the Cisco	N/A	O-MIC-WIND-030220/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Webex Teams client for Windows. A successful exploit could allow the attacker to cause the targeted user's client to crash continuously. This vulnerability was introduced in Cisco Webex Teams client for Windows Release 3.0.13131. **CVE ID : CVE-2020-3131**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-01-2020	9.3	Adobe Illustrator CC versions 24.0 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3710**	https://helpx.adobe.com/security/products/illustrator/apsb20-03.html	O-MIC-WIND-030220/274
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-01-2020	9.3	Adobe Illustrator CC versions 24.0 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3711**	https://helpx.adobe.com/security/products/illustrator/apsb20-03.html	O-MIC-WIND-030220/275
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-01-2020	9.3	Adobe Illustrator CC versions 24.0 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3712**	https://helpx.adobe.com/security/products/illustrator/apsb20-03.html	O-MIC-WIND-030220/276
Improper Restriction of Operations within the	29-01-2020	9.3	Adobe Illustrator CC versions 24.0 and earlier have a memory corruption vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/illustrator/apsb20-	O-MIC-WIND-030220/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			arbitrary code execution. **CVE ID : CVE-2020-3713**	03.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	29-01-2020	9.3	Adobe Illustrator CC versions 24.0 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3714**	https://helpx.adobe.com/security/products/illustrator/apsb20-03.html	O-MIC-WIND-030220/278
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-01-2020	5	tftp.c in libslirp 4.1.0, as used in QEMU 4.2.0, does not prevent ..\ directory traversal on Windows. **CVE ID : CVE-2020-7211**	http://www.openwall.com/lists/oss-security/2020/01/17/2	O-MIC-WIND-030220/279
Multitech					
conduit_mtcdt-lvw2-246a_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-01-2020	9	MultiTech Conduit MTCDT-LVW2-24XX 1.4.17-ocea-13592 devices allow remote authenticated administrators to execute arbitrary OS commands by navigating to the Debug Options page and entering shell metacharacters in the interface JSON field of the ping function. **CVE ID : CVE-2020-7594**	N/A	O-MUL-COND-030220/280
Philips					
hue_bridge_v2_firmware					
Out-of-bounds Write	23-01-2020	7.5	Philips Hue Bridge model 2.X prior to and including version 1935144020	N/A	O-PHI-HUE_-030220/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contains a Heap-based Buffer Overflow when handling a long ZCL string during the commissioning phase, resulting in a remote code execution. **CVE ID : CVE-2020-6007**		
Ruckuswireless					
r310_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-01-2020	3.5	Ruckus ZoneFlex R310 104.0.0.0.1347 devices allow Stored XSS via the SSID field on the Configuration > Radio 2.4G > Wireless X screen (after a successful login to the super account). **CVE ID : CVE-2020-7234**	N/A	O-RUC-R310-030220/282
SMC					
d3g0804_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-01-2020	3.5	SMC D3G0804W 3.5.2.5-LAT_GA devices allow XSS via the SSID field on the WiFi Network Configuration page (after a successful login to the admin account). **CVE ID : CVE-2020-7249**	N/A	O-SMC-D3G0-030220/283
sonoff					
th10_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site	21-01-2020	3.5	Sonoff TH 10 and 16 devices with firmware 6.6.0.21 allows XSS via the Friendly Name 1 field (after a successful login with the Web Admin Password). **CVE ID : CVE-2020-7470**	N/A	O-SON-TH10-030220/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
th16_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-01-2020	3.5	Sonoff TH 10 and 16 devices with firmware 6.6.0.21 allows XSS via the Friendly Name 1 field (after a successful login with the Web Admin Password). **CVE ID : CVE-2020-7470**	N/A	O-SON-TH16-030220/285
uhp					
uhp-100_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-01-2020	4.3	UHP UHP-100 3.4.1.15, 3.4.2.4, and 3.4.3 devices allow XSS via cB3?ta= (profile title). **CVE ID : CVE-2020-7235**	N/A	O-UHP-UHP--030220/286
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-01-2020	4.3	UHP UHP-100 3.4.1.15, 3.4.2.4, and 3.4.3 devices allow XSS via cw2?td= (Site Name field of the Site Setup section). **CVE ID : CVE-2020-7236**	N/A	O-UHP-UHP--030220/287
Westermo					
mrd-315_firmware					
Information Exposure	18-01-2020	4	Westermo MRD-315 1.7.3 and 1.7.4 devices have an information disclosure vulnerability that allows an authenticated remote attacker to retrieve the source code of different functions of the web	N/A	O-WES-MRD--030220/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application via requests that lack certain mandatory parameters. This affects ifaces-diag.asp, system.asp, backup.asp, sys-power.asp, ifaces-wls.asp, ifaces-wls-pkt.asp, and ifaces-wls-pkt-adv.asp. **CVE ID : CVE-2020-7227**		
ZTE					
f6x2w_firmware					
Information Exposure	17-01-2020	5	V6.0.10P2T2 and V6.0.10P2T5 of F6x2W product are impacted by Information leak vulnerability. Unauthorized users could log in directly to obtain page information without entering a verification code. **CVE ID : CVE-2020-6862**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1012162	O-ZTE-F6X2-030220/289
Hardware					
a1					
wlan_box_adb_vv2220					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-01-2020	3.5	The Username field in the Storage Service settings of A1 WLAN Box ADB VV2220v2 devices allows stored XSS (after a successful Administrator login). **CVE ID : CVE-2020-8090**	N/A	H-A1-WLAN-030220/290
Arris					
ruckus_zoneflex_r500					
Improper Neutralization of Special	29-01-2020	9	Ruckus ZoneFlex R500 104.0.0.0.1347 devices allow an authenticated	N/A	H-ARR-RUCK-030220/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			attacker to execute arbitrary OS commands via the hidden /forms/nslookupHandler form, as demonstrated by the nslookuptarget=|cat${IFS} substring. **CVE ID : CVE-2020-8438**		
Asus					
rt-ac66u					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-01-2020	4.3	ASUS WRT-AC66U 3 RT 3.0.0.4.372_67 devices allow XSS via the Client Name field to the Parental Control feature. **CVE ID : CVE-2020-7997**	N/A	H-ASU-RT-A-030220/292
Cisco					
sg250-08					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to	N/A	H-CIS-SG25-030220/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-08hp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG25-030220/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg250-10p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG25-030220/295
sg250-18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability	N/A	H-CIS-SG25-030220/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-26					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could	N/A	H-CIS-SG25-030220/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sg250-26hp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG25-030220/298
sg250-26p					
Improper Neutralizatio	26-01-2020	4.3	A vulnerability in the web-based management	N/A	H-CIS-SG25-030220/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-50					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based	N/A	H-CIS-SG25-030220/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-50hp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the	N/A	H-CIS-SG25-030220/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sg250-50p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG25-030220/302
sg250x-24					
Improper Neutralization of Input During Web Page	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could	N/A	H-CIS-SG25-030220/303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250x-24p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this	N/A	H-CIS-SG25-030220/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250x-48					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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.	N/A	H-CIS-SG25-030220/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3121		
sg250x-48p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG25-030220/306
sf350-48					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the	N/A	H-CIS-SF35-030220/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sf350-48mp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A	N/A	H-CIS-SF35-030220/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sf350-48p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SF35-030220/309
sg350-10					
Improper	26-01-2020	4.3	A vulnerability in the web-	N/A	H-CIS-SG35-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		030220/310
sg350-10mp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied	N/A	H-CIS-SG35-030220/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg350-10p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could allow the attacker to execute arbitrary script	N/A	H-CIS-SG35-030220/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sg350-28					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG35-030220/313
sg350-28mp					
Improper Neutralization of Input During Web	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and	N/A	H-CIS-SG35-030220/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg350-28p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An	N/A	H-CIS-SG35-030220/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sf550x-24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based	N/A	H-CIS-SF55-030220/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information. **CVE ID : CVE-2020-3121**		
sf550x-24p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SF55-030220/317
sf550x-48					
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct	N/A	H-CIS-SF55-030220/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sf550x-48mp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to	N/A	H-CIS-SF55-030220/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sf550x-48p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SF55-030220/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg200-08					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG20-030220/321
sg200-08p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful	N/A	H-CIS-SG20-030220/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-10fp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG20-030220/323
sg200-18					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on	N/A	H-CIS-SG20-030220/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-26					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18	N/A	H-CIS-SG20-030220/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3147		
sg200-26fp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG20-030220/326
sg200-26p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an	N/A	H-CIS-SG20-030220/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-50					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG20-030220/328
sg200-50fp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of	N/A	H-CIS-SG20-030220/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-50p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases	N/A	H-CIS-SG20-030220/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf300-08					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SF30-030220/331
sf300-24					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by	N/A	H-CIS-SF30-030220/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf300-24mp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SF30-030220/333
sf300-24p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an	N/A	H-CIS-SF30-030220/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf300-24pp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS	N/A	H-CIS-SF30-030220/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf300-48					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SF30-030220/336
sf300-48p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web	N/A	H-CIS-SF30-030220/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf300-48pp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SF30-030220/338
sf302-08					
Improper	30-01-2020	7.8	A vulnerability in the web	N/A	H-CIS-SF30-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		030220/339
sf302-08mp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an	N/A	H-CIS-SF30-030220/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf302-08mpp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SF30-030220/341
sf302-08p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to	N/A	H-CIS-SF30-030220/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf302-08pp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SF30-030220/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-10					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG30-030220/344
sg300-10mp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful	N/A	H-CIS-SG30-030220/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-10mpp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG30-030220/346
sg300-10p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on	N/A	H-CIS-SG30-030220/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-10pp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18	N/A	H-CIS-SG30-030220/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3147		
sg300-10sfp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG30-030220/349
sg300-20					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an	N/A	H-CIS-SG30-030220/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-28					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG30-030220/351
sg300-28mp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of	N/A	H-CIS-SG30-030220/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-28p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases	N/A	H-CIS-SG30-030220/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg250-24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG25-030220/354
sg250-24p					
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct	N/A	H-CIS-SG25-030220/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-48					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to	N/A	H-CIS-SG25-030220/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg250-48hp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG25-030220/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg355-10mp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG35-030220/358
sx550x-12ft					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability	N/A	H-CIS-SX55-030220/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg200-24					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases	N/A	H-CIS-SG20-030220/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-24p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG20-030220/361
sg200-24fp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by	N/A	H-CIS-SG20-030220/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg200-48					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG20-030220/363
sg200-48p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an	N/A	H-CIS-SG20-030220/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg550x-24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and	N/A	H-CIS-SG55-030220/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg550x-24mp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG55-030220/366
sg550x-24mpp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG55-030220/367
sg550x-24p					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient	N/A	H-CIS-SG55-030220/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sg550x-48					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could allow the attacker to	N/A	H-CIS-SG55-030220/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sg550x-48mp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SG55-030220/370
sg550x-48p					
Improper Neutralization of Input	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small	N/A	H-CIS-SG55-030220/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sx550x-16ft					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of	N/A	H-CIS-SX55-030220/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
sx550x-24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access	N/A	H-CIS-SX55-030220/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive, browser-based information. **CVE ID : CVE-2020-3121**		
sx550x-24ft					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**	N/A	H-CIS-SX55-030220/374
sx550x-52					
Improper Neutralization of Input During Web Page Generation	26-01-2020	4.3	A vulnerability in the web-based management interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	H-CIS-SX55-030220/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link and access a specific page. 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. **CVE ID : CVE-2020-3121**		
vedge-100					
Improper Privilege Management	26-01-2020	7.2	A vulnerability in the CLI of the Cisco SD-WAN Solution vManage software could allow an authenticated, local attacker to elevate privileges to root-level privileges on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted file to the affected system. An exploit could allow the attacker to elevate privileges to root-level privileges.	N/A	H-CIS-VEDG-030220/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3115		
vedge-1000					
Improper Privilege Management	26-01-2020	7.2	A vulnerability in the CLI of the Cisco SD-WAN Solution vManage software could allow an authenticated, local attacker to elevate privileges to root-level privileges on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted file to the affected system. An exploit could allow the attacker to elevate privileges to root-level privileges. **CVE ID : CVE-2020-3115**	N/A	H-CIS-VEDG-030220/377
vedge-2000					
Improper Privilege Management	26-01-2020	7.2	A vulnerability in the CLI of the Cisco SD-WAN Solution vManage software could allow an authenticated, local attacker to elevate privileges to root-level privileges on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted file to the affected system. An exploit could allow the attacker to elevate privileges to root-level privileges. **CVE ID : CVE-2020-3115**	N/A	H-CIS-VEDG-030220/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vedge-5000					
Improper Privilege Management	26-01-2020	7.2	A vulnerability in the CLI of the Cisco SD-WAN Solution vManage software could allow an authenticated, local attacker to elevate privileges to root-level privileges on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted file to the affected system. An exploit could allow the attacker to elevate privileges to root-level privileges. **CVE ID : CVE-2020-3115**	N/A	H-CIS-VEDG-030220/379
vedge-100b					
Improper Privilege Management	26-01-2020	7.2	A vulnerability in the CLI of the Cisco SD-WAN Solution vManage software could allow an authenticated, local attacker to elevate privileges to root-level privileges on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted file to the affected system. An exploit could allow the attacker to elevate privileges to root-level privileges. **CVE ID : CVE-2020-3115**	N/A	H-CIS-VEDG-030220/380
vedge_100m					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	26-01-2020	7.2	A vulnerability in the CLI of the Cisco SD-WAN Solution vManage software could allow an authenticated, local attacker to elevate privileges to root-level privileges on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted file to the affected system. An exploit could allow the attacker to elevate privileges to root-level privileges. **CVE ID : CVE-2020-3115**	N/A	H-CIS-VEDG-030220/381
vedge_100wm					
Improper Privilege Management	26-01-2020	7.2	A vulnerability in the CLI of the Cisco SD-WAN Solution vManage software could allow an authenticated, local attacker to elevate privileges to root-level privileges on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted file to the affected system. An exploit could allow the attacker to elevate privileges to root-level privileges. **CVE ID : CVE-2020-3115**	N/A	H-CIS-VEDG-030220/382
sg300-28pp					
Improper	30-01-2020	7.8	A vulnerability in the web	N/A	H-CIS-SG30-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		030220/383
sg300-52					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an	N/A	H-CIS-SG30-030220/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg300-52mp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG30-030220/385
sg300-52p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to	N/A	H-CIS-SG30-030220/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf500-24					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SF50-030220/387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf500-24p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SF50-030220/388
sf500-48					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful	N/A	H-CIS-SF50-030220/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sf500-48p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SF50-030220/390
sg500-28					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on	N/A	H-CIS-SG50-030220/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg500-28mpp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18	N/A	H-CIS-SG50-030220/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3147		
sg500-28p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG50-030220/393
sg500-52					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an	N/A	H-CIS-SG50-030220/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg500-52mp					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG50-030220/395
sg500-52p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of	N/A	H-CIS-SG50-030220/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg500x-24					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases	N/A	H-CIS-SG50-030220/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg500x-24p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG50-030220/398
sg500x-48					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by	N/A	H-CIS-SG50-030220/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
sg500x-48p					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**	N/A	H-CIS-SG50-030220/400
sg500xg-8f8t					
Improper Input Validation	30-01-2020	7.8	A vulnerability in the web UI of Cisco Small Business Switches could allow an	N/A	H-CIS-SG50-030220/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition. This vulnerability affects firmware releases prior than 1.3.7.18 **CVE ID : CVE-2020-3147**		
comtechtel					
stampede_fx-1010					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-01-2020	9	Comtech Stampede FX-1010 7.4.3 devices allow remote authenticated administrators to achieve remote code execution by navigating to the Diagnostics Trace Route page and entering shell metacharacters in the Target IP address field. (In some cases, authentication can be achieved with the comtech password for the comtech account.) **CVE ID : CVE-2020-7242**	N/A	H-COM-STAM-030220/402
Improper Neutralizatio	20-01-2020	9	Comtech Stampede FX-1010 7.4.3 devices allow remote	N/A	H-COM-STAM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			authenticated administrators to achieve remote code execution by navigating to the Fetch URL page and entering shell metacharacters in the URL field. (In some cases, authentication can be achieved with the comtech password for the comtech account.) **CVE ID : CVE-2020-7243**		030220/403
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-01-2020	9	Comtech Stampede FX-1010 7.4.3 devices allow remote authenticated administrators to achieve remote code execution by navigating to the Poll Routes page and entering shell metacharacters in the Router IP Address field. (In some cases, authentication can be achieved with the comtech password for the comtech account.) **CVE ID : CVE-2020-7244**	N/A	H-COM-STAM-030220/404
Eaton					
5p_850					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-01-2020	3.5	An issue was discovered on Eaton 5P 850 devices. The Ubicacion SAI field allows XSS attacks by an administrator. **CVE ID : CVE-2020-7915**	N/A	H-EAT-5P_8-030220/405
Huawei					
honor_v30					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	21-01-2020	4.3	Honor V30 smartphones with versions earlier than 10.0.1.135(C00E130R4P1) have an improper authentication vulnerability. Certain applications do not properly validate the identity of another application who would call its interface. An attacker could trick the user into installing a malicious application. Successful exploit could allow unauthorized actions leading to information disclosure. **CVE ID : CVE-2020-1788**	N/A	H-HUA-HONO-030220/406
mate_20					
Improper Authentication	21-01-2020	3.6	HUAWEI Mate 20 smart phones with versions earlier than 10.0.0.175(C00E70R3P8) have an insufficient authentication vulnerability. A local attacker with high privilege can execute a specific command to exploit this vulnerability. Successful exploitation may cause information leak and compromise the availability of the smart phones.Affected product versions include: HUAWEI Mate 20 versions Versions earlier than 10.0.0.175(C00E70R3P8)	N/A	H-HUA-MATE-030220/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1840		
kmccontrols					
bac-a1616bc					
Use of Hard-coded Credentials	19-01-2020	10	KMS Controls BAC-A1616BC BACnet devices have a cleartext password of snowman in the BACKDOOR_NAME variable in the BC_Logon.swf file. **CVE ID : CVE-2020-7233**	N/A	H-KMC-BAC--030220/408
meinbergglobal					
lantime_m300					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-01-2020	9	Meinberg Lantime M300 and M1000 devices allow attackers (with privileges to configure a device) to execute arbitrary OS commands by editing the /config/netconf.cmd script (aka Extended Network Configuration). **CVE ID : CVE-2020-7240**	N/A	H-MEI-LANT-030220/409
lantime_m1000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-01-2020	9	Meinberg Lantime M300 and M1000 devices allow attackers (with privileges to configure a device) to execute arbitrary OS commands by editing the /config/netconf.cmd script (aka Extended Network Configuration). **CVE ID : CVE-2020-7240**	N/A	H-MEI-LANT-030220/410
Multitech					
conduit_mtcdt-lvw2-246a					
Improper Neutralizatio	21-01-2020	9	MultiTech Conduit MTCDT-LVW2-24XX 1.4.17-ocea-	N/A	H-MUL-COND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			13592 devices allow remote authenticated administrators to execute arbitrary OS commands by navigating to the Debug Options page and entering shell metacharacters in the interface JSON field of the ping function. **CVE ID : CVE-2020-7594**		030220/411
Philips					
hue_bridge_v2					
Out-of-bounds Write	23-01-2020	7.5	Philips Hue Bridge model 2.X prior to and including version 1935144020 contains a Heap-based Buffer Overflow when handling a long ZCL string during the commissioning phase, resulting in a remote code execution. **CVE ID : CVE-2020-6007**	N/A	H-PHI-HUE_-030220/412
Ruckuswireless					
r310					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-01-2020	3.5	Ruckus ZoneFlex R310 104.0.0.0.1347 devices allow Stored XSS via the SSID field on the Configuration > Radio 2.4G > Wireless X screen (after a successful login to the super account). **CVE ID : CVE-2020-7234**	N/A	H-RUC-R310-030220/413
SMC					
d3g0804					
Improper Neutralizatio	21-01-2020	3.5	SMC D3G0804W 3.5.2.5-LAT_GA devices allow XSS	N/A	H-SMC-D3G0-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			via the SSID field on the WiFi Network Configuration page (after a successful login to the admin account). **CVE ID : CVE-2020-7249**		030220/414
sonoff					
th10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-01-2020	3.5	Sonoff TH 10 and 16 devices with firmware 6.6.0.21 allows XSS via the Friendly Name 1 field (after a successful login with the Web Admin Password). **CVE ID : CVE-2020-7470**	N/A	H-SON-TH10-030220/415
th16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-01-2020	3.5	Sonoff TH 10 and 16 devices with firmware 6.6.0.21 allows XSS via the Friendly Name 1 field (after a successful login with the Web Admin Password). **CVE ID : CVE-2020-7470**	N/A	H-SON-TH16-030220/416
uhp					
uhp-100					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-01-2020	4.3	UHP UHP-100 3.4.1.15, 3.4.2.4, and 3.4.3 devices allow XSS via cB3?ta= (profile title). **CVE ID : CVE-2020-7235**	N/A	H-UHP-UHP--030220/417
Improper Neutralization of Input	19-01-2020	4.3	UHP UHP-100 3.4.1.15, 3.4.2.4, and 3.4.3 devices allow XSS via cw2?td= (Site	N/A	H-UHP-UHP--030220/418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Name field of the Site Setup section). **CVE ID : CVE-2020-7236**		
Westermo					
mrd-315					
Information Exposure	18-01-2020	4	Westermo MRD-315 1.7.3 and 1.7.4 devices have an information disclosure vulnerability that allows an authenticated remote attacker to retrieve the source code of different functions of the web application via requests that lack certain mandatory parameters. This affects ifaces-diag.asp, system.asp, backup.asp, sys-power.asp, ifaces-wls.asp, ifaces-wls-pkt.asp, and ifaces-wls-pkt-adv.asp. **CVE ID : CVE-2020-7227**	N/A	H-WES-MRD--030220/419
ZTE					
f6x2w					
Information Exposure	17-01-2020	5	V6.0.10P2T2 and V6.0.10P2T5 of F6x2W product are impacted by Information leak vulnerability. Unauthorized users could log in directly to obtain page information without entering a verification code. **CVE ID : CVE-2020-6862**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1012162	H-ZTE-F6X2-030220/420