https://nciipc.gov.in

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 - 31 May 2021 Vol. 08 No. 10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
acymailing					
acymailing					
URL Redirection to Untrusted Site ('Open Redirect')	17-May-21	5.8	When subscribing using AcyMailing, the 'redirect' parameter isn't properly sanitized. Turning the request from POST to GET, an attacker can craft a link containing a potentially malicious landing page and send it to the victim. **CVE ID : CVE-2021-24288**	https://wpscan.com/vulnerability/56628862-1687-4862-9ed4-145d8dfbca97	A-ACY-ACYM-040621/1
Admidio					
admidio					
Unrestricted Upload of File with Dangerous Type	20-May-21	6.5	Admidio is a free, open source user management system for websites of organizations and groups. In Admidio before version 4.0.4, there is an authenticated RCE via .phar file upload. A php web shell can be uploaded via the Documents & Files upload feature. Someone with upload permissions could rename the php shell with a .phar extension, visit the file, triggering the payload for a reverse/bind shell. This can be mitigated by excluding a .phar file extension to be uploaded (like you did with .php .phtml .php5 etc). The vulnerability is patched in	https://github.com/Admidio/admidio/security/advisories/GHSA-xpqj-67r8-25j2	A-ADM-ADMI-040621/2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 4.0.4. **CVE ID : CVE-2021-32630**		
adminer					
adminer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-21	4.3	Adminer is open-source database management software. A cross-site scripting vulnerability in Adminer versions 4.6.1 to 4.8.0 affects users of MySQL, MariaDB, PgSQL and SQLite. XSS is in most cases prevented by strict CSP in all modern browsers. The only exception is when Adminer is using a `pdo_` extension to communicate with the database (it is used if the native extensions are not enabled). In browsers without CSP, Adminer versions 4.6.1 to 4.8.0 are affected. The vulnerability is patched in version 4.8.1. As workarounds, one can use a browser supporting strict CSP or enable the native PHP extensions (e.g. `mysqli`) or disable displaying PHP errors (`display_errors`). **CVE ID : CVE-2021-29625**	https://github.com/vrana/adminer/commit/4043092ec2c0de2258d60a99d0c5958637d051a7, https://github.com/vrana/adminer/security/advisories/GHSA-2v82-5746-vwqc	A-ADM-ADMI-040621/3
aioseo					
all_in_one_seo					
Improper Control of Generation of Code ('Code	24-May-21	9	The All in One SEO – Best WordPress SEO Plugin – Easily Improve Your SEO Rankings before 4.1.0.2 enables authenticated users with "aioseo_tools_settings"	https://wpscan.com/vulnerability/ab2c94d2-f6c4-418b-bd14-711ed164bcf	A-AIO-ALL_-040621/4

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
Injection')		🟥	privilege (most of the time admin) to execute arbitrary code on the underlying host. Users can restore plugin's configuration by uploading a backup .ini file in the section "Tool > Import/Export". However, the plugin attempts to unserialize values of the .ini file. Moreover, the plugin embeds Monolog library which can be used to craft a gadget chain and thus trigger system command execution. **CVE ID : CVE-2021-24307**	1, https://aioseo.com/changelog/	
arangodb					
arangodb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	4.3	In ArangoDB, versions v2.2.6.2 through v3.7.10 are vulnerable to Cross-Site Scripting (XSS), since there is no validation of the .zip file name and filtering of potential abusive characters which zip files can be named to. There is no X-Frame-Options Header set, which makes it more susceptible for leveraging self XSS by attackers. **CVE ID : CVE-2021-25938**	https://github.com/arangodb/arangodb/commit/3e486b9bc33cc97e92645dd279899000e57f61f4	A-ARA-ARAN-040621/5
autoptimize					
autoptimize					
Improper Neutralization of Input During Web Page Generation ('Cross-site	24-May-21	3.5	The Autoptimize WordPress plugin before 2.8.4 was missing proper escaping and sanitisation in some of its settings, allowing high privilege users to set XSS payloads in them, leading to	https://wpscan.com/vulnerability/6678e064-ce21-4bb2-8c50-061073fb22f	A-AUT-AUTO-040621/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			stored Cross-Site Scripting issues **CVE ID : CVE-2021-24332**	b	
Bitdefender					
endpoint_security_tools					
Improper Input Validation	24-May-21	6	An Improper Input Validation vulnerability in the Product Update feature of Bitdefender Endpoint Security Tools for Linux allows a man-in-the-middle attacker to abuse the DownloadFile function of the Product Update to achieve remote code execution. This issue affects: Bitdefender Endpoint Security Tools for Linux versions prior to 6.2.21.155. **CVE ID : CVE-2021-3485**	https://www.bitdefender.com/support/security-advisories/improper-input-validation-in-bitdefender-endpoint-security-tools-for-linux-va-9769	A-BIT-ENDP-040621/7
gravityzone_business_security					
Uncontrolled Search Path Element	18-May-21	4.6	Uncontrolled Search Path Element vulnerability in the openssl component as used in Bitdefender GravityZone Business Security allows an attacker to load a third party DLL to elevate privileges. This issue affects Bitdefender GravityZone Business Security versions prior to 6.6.23.329. **CVE ID : CVE-2021-3423**	https://www.bitdefender.com/support/security-advisories/privilege-escalation-in-bitdefender-gravityzone-business-security-va-9557	A-BIT-GRAV-040621/8
bluemedicinelabs					
hotjar_connecticator					
Improper Neutralizatio	24-May-21	3.5	The Hotjar Connecticator WordPress plugin through	https://wpscan.com/vuln	A-BLU-HOTJ-040621/9

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
n of Input During Web Page Generation ('Cross-site Scripting')			1.1.1 is vulnerable to Stored Cross-Site Scripting (XSS) in the 'hotjar script' textarea. The request did include a CSRF nonce that was properly verified by the server and this vulnerability could only be exploited by administrator users. **CVE ID : CVE-2021-24301**	erability/eb8e2b9d-f153-49c9-862a-5c016934f9ad	
boostifythemes					
goto					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	4.3	The Goto WordPress theme before 2.1 did not properly sanitize the formvalue JSON POST parameter in its tl_filter AJAX action, leading to an unauthenticated Reflected Cross-site Scripting (XSS) vulnerability. **CVE ID : CVE-2021-24297**	https://wpscan.com/vulnerability/a64a3b2e-7924-47aa-96e8-3aa02a6cdccc	A-BOO-GOTO-040621/10
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-21	7.5	The Goto WordPress theme before 2.1 did not sanitise, validate of escape the keywords GET parameter from its listing page before using it in a SQL statement, leading to an Unauthenticated SQL injection issue **CVE ID : CVE-2021-24314**	https://wpscan.com/vulnerability/1cc6dc17-b019-49dd-8149-c8bba165eb30	A-BOO-GOTO-040621/11
calendar01_project					
calendar01					
Improper Neutralization of Input During Web Page Generation	24-May-21	4.3	Reflected cross-site scripting vulnerability in the admin page of [Calendar01] free edition ver1.0.1 and earlier allows a remote attacker to inject an arbitrary script via	N/A	A-CAL-CALE-040621/12

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')			unspecified vectors. **CVE ID : CVE-2021-20725**		
catzsoft					
redi_restaurant_reservation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	The ReDi Restaurant Reservation WordPress plugin before 21.0426 provides the functionality to let users make restaurant reservations. These reservations are stored and can be listed on an 'Upcoming' page provided by the plugin. An unauthenticated user can fill in the form to make a restaurant reservation. The form to make a restaurant reservation field called 'Comment' does not use proper input validation and can be used to store XSS payloads. The XSS payloads will be executed when the plugin user goes to the 'Upcoming' page, which is an external website https://upcoming.reservationdiary.eu/ loaded in an iframe, and the stored reservation with XSS payload is loaded. **CVE ID : CVE-2021-24299**	https://wpscan.com/vulnerability/fd6ce00b-8c5f-4180-b648-f47b37303670	A-CAT-REDI-040621/13
centos-webpanel					
centos_web_panel					
Improper Neutralization of Special Elements used in an SQL	18-May-21	10	The unprivileged user portal part of CentOS Web Panel is affected by a SQL Injection via the 'idsession' HTTP POST parameter.	N/A	A-CEN-CENT-040621/14

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
Command ('SQL Injection')			**CVE ID : CVE-2021-31316**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-May-21	10	The unprivileged user portal part of CentOS Web Panel is affected by a Command Injection vulnerability leading to root Remote Code Execution. **CVE ID : CVE-2021-31324**	N/A	A-CEN-CENT-040621/15
Centreon					
centreon					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-May-21	3.5	Centreon version 20.10.2 is affected by a cross-site scripting (XSS) vulnerability. The dep_description (Dependency Description) and dep_name (Dependency Name) parameters are vulnerable to stored XSS. A user has to log in and go to the Configuration > Notifications > Hosts page. **CVE ID : CVE-2021-27676**	https://github.com/centreon/centreon/pull/9587, http://centreon.com	A-CEN-CENT-040621/16
cesnet					
libyang					
Unchecked Return Value	20-May-21	5	In function read_yin_container() in libyang <= v1.0.225, it doesn't check whether the value of retval->ext[r] is NULL. In some cases, it can be NULL, which leads to the operation of retval->ext[r]->flags that results in a crash. **CVE ID : CVE-2021-28902**	https://github.com/CESNET/libyang/issues/1454	A-CES-LIBY-040621/17
Uncontrolled	20-May-21	5	A stack overflow in libyang <=	https://githu	A-CES-LIBY-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Recursion			v1.0.225 can cause a denial of service through function lyxml_parse_mem(). lyxml_parse_elem() function will be called recursively, which will consume stack space and lead to crash. **CVE ID : CVE-2021-28903**	b.com/CESNET/libyang/issues/1453	040621/18
Unchecked Return Value	20-May-21	5	In function ext_get_plugin() in libyang <= v1.0.225, it doesn't check whether the value of revision is NULL. If revision is NULL, the operation of strcmp(revision, ext_plugins[u].revision) will lead to a crash. **CVE ID : CVE-2021-28904**	https://github.com/CESNET/libyang/issues/1451	A-CES-LIBY-040621/19
Reachable Assertion	20-May-21	5	In function lys_node_free() in libyang <= v1.0.225, it asserts that the value of node->module can't be NULL. But in some cases, node->module can be null, which triggers a reachable assertion (CWE-617). **CVE ID : CVE-2021-28905**	https://github.com/CESNET/libyang/issues/1452	A-CES-LIBY-040621/20
Unchecked Return Value	20-May-21	5	In function read_yin_leaf() in libyang <= v1.0.225, it doesn't check whether the value of retval->ext[r] is NULL. In some cases, it can be NULL, which leads to the operation of retval->ext[r]->flags that results in a crash. **CVE ID : CVE-2021-28906**	https://github.com/CESNET/libyang/issues/1455	A-CES-LIBY-040621/21
Cisco					
dna_spaces\					
Improper	22-May-21	7.2	Multiple vulnerabilities in	https://tools.	A-CIS-DNA_-

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
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. These vulnerabilities are due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities by leveraging the insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin and execute arbitrary commands on the underlying operating system as root. **CVE ID : CVE-2021-1557**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnasp-conn-prvesc-q6T6BzW	040621/22
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-May-21	7.2	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. These vulnerabilities are due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities by leveraging the insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnasp-conn-prvesc-q6T6BzW	A-CIS-DNA_-040621/23

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
			and execute arbitrary commands on the underlying operating system as root. **CVE ID : CVE-2021-1558**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-May-21	9	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, remote attacker to perform a command injection attack on an affected device. These vulnerabilities are due to insufficient input sanitization when executing affected commands. A high-privileged attacker could exploit these vulnerabilities on a Cisco DNA Spaces Connector by injecting crafted input during command execution. A successful exploit could allow the attacker to execute arbitrary commands as root within the Connector docker container. **CVE ID : CVE-2021-1559**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnasp-conn-cmdinj-HOj4YV5n	A-CIS-DNA_-040621/24
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-May-21	9	Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, remote attacker to perform a command injection attack on an affected device. These vulnerabilities are due to insufficient input sanitization when executing affected commands. A high-privileged attacker could exploit these vulnerabilities on a Cisco DNA Spaces Connector by injecting crafted input during command execution. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnasp-conn-cmdinj-HOj4YV5n	A-CIS-DNA_-040621/25

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands as root within the Connector docker container. **CVE ID : CVE-2021-1560**		
evolved_programmable_network_manager					
Externally Controlled Reference to a Resource in Another Sphere	22-May-21	3.6	A vulnerability in the restricted shell of Cisco Evolved Programmable Network (EPN) Manager, Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to identify directories and write arbitrary files to the file system. This vulnerability is due to improper validation of parameters that are sent to a CLI command within the restricted shell. An attacker could exploit this vulnerability by logging in to the device and issuing certain CLI commands. A successful exploit could allow the attacker to identify file directories on the affected device and write arbitrary files to the file system on the affected device. To exploit this vulnerability, the attacker must be an authenticated shell user. **CVE ID : CVE-2021-1306**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ade-xcvAQEOZ	A-CIS-EVOL-040621/26
Improper Neutralization of Special Elements used in an OS Command ('OS	22-May-21	9	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Evolved Programmable Network (EPN) Manager could allow an authenticated, remote attacker to execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-	A-CIS-EVOL-040621/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			arbitrary commands on an affected system. The vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the interface. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system (OS) with the permissions of a special non-root user. In this way, an attacker could take control of the affected system, which would allow them to obtain and alter sensitive data. The attacker could also affect the devices that are managed by the affected system by pushing arbitrary configuration files, retrieving device credentials and confidential information, and ultimately undermining the stability of the devices, causing a denial of service (DoS) condition. **CVE ID : CVE-2021-1487**	cmd-inj-YU5e6tB3	
finesse					
Improper Neutralization of Input During Web Page Generation ('Cross-site	22-May-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Finesse could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-	A-CIS-FINE-040621/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit these vulnerabilities by injecting malicious code into the web-based management interface and 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 access sensitive, browser-based information. An attacker needs valid administrator credentials to inject the malicious script code. **CVE ID : CVE-2021-1254**	strd-xss-bUKqffFW	
URL Redirection to Untrusted Site ('Open Redirect')	22-May-21	5.8	A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to redirect a user to an undesired web page. This vulnerability is due to improper input validation of the URL parameters in an HTTP request that is sent to an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to cause the interface to redirect the user to a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-opn-rdrct-epDeh7R	A-CIS-FINE-040621/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific, malicious URL. This type of vulnerability is known as an open redirect and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2021-1358**		
identity_services_engine					
Externally Controlled Reference to a Resource in Another Sphere	22-May-21	3.6	A vulnerability in the restricted shell of Cisco Evolved Programmable Network (EPN) Manager, Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to identify directories and write arbitrary files to the file system. This vulnerability is due to improper validation of parameters that are sent to a CLI command within the restricted shell. An attacker could exploit this vulnerability by logging in to the device and issuing certain CLI commands. A successful exploit could allow the attacker to identify file directories on the affected device and write arbitrary files to the file system on the affected device. To exploit this vulnerability, the attacker must be an authenticated shell user. **CVE ID : CVE-2021-1306**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ade-xcvAQEOZ	A-CIS-IDEN-040621/30
modeling_labs					
Improper Neutralizatio	22-May-21	9	A vulnerability in the web UI of Cisco Modeling Labs could	https://tools.cisco.com/se	A-CIS-MODE-040621/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Argument Delimiters in a Command ('Argument Injection')			allow an authenticated, remote attacker to execute arbitrary commands with the privileges of the web application on the underlying operating system of an affected Cisco Modeling Labs server. This vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected server. A successful exploit could allow the attacker to execute arbitrary commands with the privileges of the web application, virl2, on the underlying operating system of the affected server. To exploit this vulnerability, the attacker must have valid user credentials on the web UI. **CVE ID : CVE-2021-1531**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-cml-cmd-inject-N4VYeQXB	
prime_infrastructure					
Externally Controlled Reference to a Resource in Another Sphere	22-May-21	3.6	A vulnerability in the restricted shell of Cisco Evolved Programmable Network (EPN) Manager, Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to identify directories and write arbitrary files to the file system. This vulnerability is due to improper validation of parameters that are sent to a CLI command within the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ade-xcvAQEOZ	A-CIS-PRIM-040621/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restricted shell. An attacker could exploit this vulnerability by logging in to the device and issuing certain CLI commands. A successful exploit could allow the attacker to identify file directories on the affected device and write arbitrary files to the file system on the affected device. To exploit this vulnerability, the attacker must be an authenticated shell user. **CVE ID : CVE-2021-1306**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-May-21	9	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Evolved Programmable Network (EPN) Manager could allow an authenticated, remote attacker to execute arbitrary commands on an affected system. The vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the interface. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system (OS) with the permissions of a special non-root user. In this way, an attacker could take control of the affected system, which would allow them to obtain and alter sensitive data. The	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-cmd-inj-YU5e6tB3	A-CIS-PRIM-040621/33

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could also affect the devices that are managed by the affected system by pushing arbitrary configuration files, retrieving device credentials and confidential information, and ultimately undermining the stability of the devices, causing a denial of service (DoS) condition. **CVE ID : CVE-2021-1487**		
cleantalk					
spam_protection\\,_antispam\\,_firewall					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-21	5	It was possible to exploit an Unauthenticated Time-Based Blind SQL Injection vulnerability in the Spam protection, AntiSpam, FireWall by CleanTalk WordPress Plugin before 5.153.4. The update_log function in lib/Cleantalk/ApbctWP/Firewall/SFW.php included a vulnerable query that could be injected via the User-Agent Header by manipulating the cookies set by the Spam protection, AntiSpam, FireWall by CleanTalk WordPress plugin before 5.153.4, sending an initial request to obtain a ct_sfw_pass_key cookie and then manually setting a separate ct_sfw_passed cookie and disallowing it from being reset.	https://wpscan.com/vulnerability/152171fc-888c-4275-a118-5a1e664ef28b	A-CLE-SPAM-040621/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24295		
clogica					
all_404_redirect_to_homepage					
Cross-Site Request Forgery (CSRF)	17-May-21	4.3	The 404 SEO Redirection WordPress plugin through 1.3 is lacking CSRF checks in all its settings, allowing attackers to make a logged in user change the plugin's settings. Due to the lack of sanitisation and escaping in some fields, it could also lead to Stored Cross-Site Scripting issues **CVE ID : CVE-2021-24324**	https://wpscan.com/vulnerability/63a24890-3735-4016-b4b7-4b070a842664	A-CLO-ALL_-040621/35
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	3.5	The tab parameter of the settings page of the All 404 Redirect to Homepage WordPress plugin before 1.21 was vulnerable to an authenticated reflected Cross-Site Scripting (XSS) issue as user input was not properly sanitised before being output in an attribute. **CVE ID : CVE-2021-24326**	https://wpscan.com/vulnerability/63d6ca03-e0df-40db-9839-531c13619094	A-CLO-ALL_-040621/36
seo_redirection_plugin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	The tab parameter of the settings page of the 404 SEO Redirection WordPress plugin through 1.3 is vulnerable to a reflected Cross-Site Scripting (XSS) issue as user input is not properly sanitised or escaped before being output in an attribute. **CVE ID : CVE-2021-24325**	https://wpscan.com/vulnerability/96e9a7fd-9ab8-478e-9420-4bca2a0b23a1	A-CLO-SEO_-040621/37
Improper Neutralizatio	17-May-21	3.5	The SEO Redirection Plugin â€“ 301 Redirect Manager	https://wpscan.com/vuln	A-CLO-SEO_-040621/38

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
n of Input During Web Page Generation ('Cross-site Scripting')			WordPress plugin before 6.4 did not sanitise the Redirect From and Redirect To fields when creating a new redirect in the dashboard, allowing high privilege users (even with the unfiltered_html disabled) to set XSS payloads **CVE ID : CVE-2021-24327**	erability/ca8068f7-dcf0-44fd-841d-d02987220d79	
Codesys					
plcwinnt					
Out-of-bounds Write	25-May-21	5	CODESYS V2 runtime system SP before 2.4.7.55 has a Heap-based Buffer Overflow. **CVE ID : CVE-2021-30186**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14725&token=08691519ef764b252630759eff925890176ecd78&download=	A-COD-PLCW-040621/39
Out-of-bounds Read	25-May-21	5	CODESYS V2 runtime system before 2.4.7.55 has Improper Input Validation. **CVE ID : CVE-2021-30195**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14725&token=08691519ef764b252630759eff925	A-COD-PLCW-040621/40

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
				890176ecd78&download=	
runtime_toolkit					
Out-of-bounds Write	25-May-21	5	CODESYS V2 runtime system SP before 2.4.7.55 has a Heap-based Buffer Overflow. **CVE ID : CVE-2021-30186**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14725&token=08691519ef764b252630759eff925890176ecd78&download=	A-COD-RUNT-040621/41
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	25-May-21	4.6	CODESYS V2 runtime system SP before 2.4.7.55 has Improper Neutralization of Special Elements used in an OS Command. **CVE ID : CVE-2021-30187**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14727&token=25159b0fc4355f4c6bc2e074a519a9d0cdb23fbb&download=	A-COD-RUNT-040621/42
Out-of-bounds Read	25-May-21	5	CODESYS V2 runtime system before 2.4.7.55 has Improper Input Validation. **CVE ID : CVE-2021-30195**	https://customers.codesys.com/index.php, https://custo	A-COD-RUNT-040621/43

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
				mers.codesys.com/index.php?eID=dumpFile&t=f&f=14725&token=08691519ef764b252630759eff925890176ecd78&download=	
v2_runtime_system_sp					
Out-of-bounds Write	25-May-21	7.5	CODESYS V2 runtime system SP before 2.4.7.55 has a Stack-based Buffer Overflow. **CVE ID : CVE-2021-30188**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14725&token=08691519ef764b252630759eff925890176ecd78&download=	A-COD-V2_R-040621/44
v2_web_server					
Out-of-bounds Write	25-May-21	7.5	CODESYS V2 Web-Server before 1.1.9.20 has a Stack-based Buffer Overflow. **CVE ID : CVE-2021-30189**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14726&token=553da5d1	A-COD-V2_W-040621/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1234bbe1ceed59969d419a71bb8c8747&download=	
Exposure of Resource to Wrong Sphere	25-May-21	7.5	CODESYS V2 Web-Server before 1.1.9.20 has Improper Access Control. **CVE ID : CVE-2021-30190**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14726&token=553da5d11234bbe1ceed59969d419a71bb8c8747&download=	A-COD-V2_W-040621/46
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-May-21	5	CODESYS V2 Web-Server before 1.1.9.20 has a a Buffer Copy without Checking the Size of the Input. **CVE ID : CVE-2021-30191**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14726&token=553da5d11234bbe1ceed59969d419a71bb8c8747&download=	A-COD-V2_W-040621/47
Incorrect Authorization	25-May-21	7.5	CODESYS V2 Web-Server before 1.1.9.20 has an Improperly Implemented	https://customers.codesys.com/index.p	A-COD-V2_W-040621/48

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
			Security Check. **CVE ID : CVE-2021-30192**	hp, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14726&token=553da5d11234bbe1ceed59969d419a71bb8c8747&download=	
Out-of-bounds Write	25-May-21	7.5	CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Write. **CVE ID : CVE-2021-30193**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14726&token=553da5d11234bbe1ceed59969d419a71bb8c8747&download=	A-COD-V2_W-040621/49
Out-of-bounds Read	25-May-21	6.4	CODESYS V2 Web-Server before 1.1.9.20 has an Out-of-bounds Read. **CVE ID : CVE-2021-30194**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14726&token=553da5d11234bbe1ce	A-COD-V2_W-040621/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ed59969d419a71bb8c8747&download=	
concerto-signage					
concerto					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-21	4.3	Persistent cross-site scripting (XSS) in the web interface of Concerto through 2.3.6 allows an unauthenticated remote attacker to introduce arbitrary JavaScript by injecting an XSS payload into the First Name or Last Name parameter upon registration. When a privileged user attempts to delete the account, the XSS payload will be executed. **CVE ID : CVE-2021-31930**	N/A	A-CON-CONC-040621/51
couchbase					
couchbase_server					
Cleartext Storage of Sensitive Information	19-May-21	5	An issue was discovered in Couchbase Server 5.x and 6.x through 6.6.1 and 7.0.0 Beta. Incorrect commands to the REST API can result in leaked authentication information being stored in cleartext in the debug.log and info.log files, and is also shown in the UI visible to administrators. **CVE ID : CVE-2021-25644**	https://www.couchbase.com/resources/security#SecurityAlerts, https://www.couchbase.com/downloads	A-COU-COUC-040621/52
Cleartext Transmission of Sensitive Information	19-May-21	4.3	An issue was discovered in Couchbase Server 6.x through 6.6.1. The Couchbase Server UI is insecurely logging session cookies in the logs.	https://www.couchbase.com/resources/security#SecurityAlert	A-COU-COUC-040621/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This allows for the impersonation of a user if the log files are obtained by an attacker before a session cookie expires. **CVE ID : CVE-2021-27924**	s, https://www.couchbase.com/downloads	
Cleartext Transmission of Sensitive Information	19-May-21	3.5	An issue was discovered in Couchbase Server 6.5.x and 6.6.x through 6.6.1. When using the View Engine and Auditing is enabled, a crash condition can (depending on a race condition) cause an internal user with administrator privileges, @ns_server, to have its credentials leaked in cleartext in the ns_server.info.log file. **CVE ID : CVE-2021-27925**	https://www.couchbase.com/resources/security#SecurityAlerts, https://www.couchbase.com/downloads	A-COU-COUC-040621/54
Incorrect Authorization	19-May-21	4	In the Query Engine in Couchbase Server 6.5.x and 6.6.x through 6.6.1, Common Table Expression queries were not correctly checking the user's permissions, allowing read-access to resources beyond what those users were explicitly allowed to access. **CVE ID : CVE-2021-31158**	https://www.couchbase.com/resources/security#SecurityAlerts, https://docs.couchbase.com/server/current/release-notes/relnotes.html	A-COU-COUC-040621/55
de-baat					
store_locator_plus					
Improper Privilege Management	17-May-21	6.5	There is functionality in the Store Locator Plus for WordPress plugin through 5.5.14 that made it possible for authenticated users to	https://wpscan.com/vulnerability/078e93cd-7cf2-4e23-8171-	A-DE--STOR-040621/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update their user meta data to become an administrator on any site using the plugin. **CVE ID : CVE-2021-24289**	58d44e354d62	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	There are several endpoints in the Store Locator Plus for WordPress plugin through 5.5.15 that could allow unauthenticated attackers the ability to inject malicious JavaScript into pages. **CVE ID : CVE-2021-24290**	https://wpscan.com/vulnerability/dc368484-f2fe-4c76-ba3d-e00e7f633719	A-DE--STOR-040621/57
deep-defaults_project					
deep-defaults					
N/A	25-May-21	7.5	Prototype pollution vulnerability in 'deep-defaults' versions 1.0.0 through 1.0.5 allows attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2021-25944**	N/A	A-DEE-DEEP-040621/58
Dell					
xtremio_management_server					
Cross-Site Request Forgery (CSRF)	21-May-21	6.8	Dell EMC XtremIO Versions prior to 6.3.3-8, contain a Cross-Site Request Forgery Vulnerability in XMS. A non-privileged attacker could potentially exploit this vulnerability, leading to a privileged victim application user being tricked into sending state-changing requests to the vulnerable application, causing unintended server operations.	https://www.dell.com/support/kbdoc/000186363	A-DEL-XTRE-040621/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21549		
deltaww					
cncsoft_screeneditor					
Out-of-bounds Read	16-May-21	7.5	Delta Industrial Automation CNCSoft ScreenEditor Versions 1.01.28 (with ScreenEditor Version 1.01.2) and prior are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to execute arbitrary code. **CVE ID : CVE-2021-22668**	N/A	A-DEL-CNCS-040621/60
dns-packet_project					
dns-packet					
Exposure of Sensitive Information to an Unauthorized Actor	20-May-21	4	This affects the package dns-packet before 5.2.2. It creates buffers with allocUnsafe and does not always fill them before forming network packets. This can expose internal application memory over unencrypted network when querying crafted invalid domain names. **CVE ID : CVE-2021-23386**	https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1295719, https://snyk.io/vuln/SNYK-JS-DNSPACKET-1293563, https://github.com/mafintosh/dns-packet/commit/25f15dd0fedc53688b25fd053ebbdffe3d5c1c56	A-DNS-DNS--040621/61
dutchcoders					
transfer.sh					
Improper Neutralizatio	24-May-21	4.3	Dutchcoders transfer.sh before 1.2.4 allows XSS via an	https://github.com/dutch	A-DUT-TRAN-

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
n of Input During Web Page Generation ('Cross-site Scripting')			inline view. **CVE ID : CVE-2021-33496**	coders/transfer.sh/pull/373, https://github.com/dutchcoders/transfer.sh/commit/9df18fdc69de2e71f30d8c1e6bfab2fda2e52eb4	040621/62
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	6.4	Dutchcoders transfer.sh before 1.2.4 allows Directory Traversal for deleting files. **CVE ID : CVE-2021-33497**	https://github.com/dutchcoders/transfer.sh/pull/373	A-DUT-TRAN-040621/63
emlog					
emlog					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-May-21	6.5	An issue was discovered in emlog 6.0.0stable. There is a SQL Injection vulnerability that can execute any SQL statement and query server sensitive data via admin/navbar.php?action=add_page. **CVE ID : CVE-2021-30081**	N/A	A-EML-EMLO-040621/64
envoyproxy					
envoy					
Integer Overflow or Wraparound	20-May-21	5	An issue was discovered in Envoy through 1.71.1. There is a remotely exploitable integer overflow in which a very large grpc-timeout value leads to unexpected timeout	https://blog.envoyproxy.io	A-ENV-ENVO-040621/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			calculations. **CVE ID : CVE-2021-28682**		
NULL Pointer Dereference	20-May-21	5	An issue was discovered in Envoy through 1.71.1. There is a remotely exploitable NULL pointer dereference and crash in TLS when an unknown TLS alert code is received. **CVE ID : CVE-2021-28683**	https://blog.envoyproxy.io	A-ENV-ENVO-040621/66
Reachable Assertion	20-May-21	5	An issue was discovered in Envoy 1.14.0. There is a remotely exploitable crash for HTTP2 Metadata, because an empty METADATA map triggers a Reachable Assertion. **CVE ID : CVE-2021-29258**	https://blog.envoyproxy.io	A-ENV-ENVO-040621/67
eterm_project					
eterm					
Improper Handling of Exceptional Conditions	20-May-21	6.5	rxvt-unicode 9.22, rxvt 2.7.10, mrxvt 0.5.4, and Eterm 0.9.7 allow (potentially remote) code execution because of improper handling of certain escape sequences (ESC G Q). A response is terminated by a newline. **CVE ID : CVE-2021-33477**	http://cvs.schmorp.de/rxvt-unicode/src/command.C?r1=1.582&r2=1.583	A-ETE-ETER-040621/68
Exiv2					
exiv2					
Uncontrolled Resource Consumption	17-May-21	4.3	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An inefficient algorithm (quadratic complexity) was found in	https://github.com/Exiv2/exiv2/pull/1657, https://github.com/Exiv2/exiv2/secur	A-EXI-EXIV-040621/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Exiv2 versions v0.27.3 and earlier. The inefficient algorithm is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. The bug is fixed in version v0.27.4. Note that this bug is only triggered when _writing_ the metadata, which is a less frequently used Exiv2 operation than _reading_ the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `rm`. **CVE ID : CVE-2021-32617**	ity/advisories/GHSA-w8mv-g8qq-36mj	
Eyesofnetwork					
eyesofnetwork					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-May-21	9	EyesOfNetwork eonweb through 5.3-11 allows Remote Command Execution (by authenticated users) via shell metacharacters in the nagios_path parameter to lilac/export.php, as demonstrated by %26%26+curl to insert an "&& curl" substring for the shell. **CVE ID : CVE-2021-33525**	N/A	A-EYE-EYES-040621/70
fastify					
fastify-csrf					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reliance on Cookies without Validation and Integrity Checking	19-May-21	4.3	fastify-csrf is an open-source plugin helps developers protect their Fastify server against CSRF attacks. Versions of fastify-csrf prior to 3.1.0 have a "double submit" mechanism using cookies with an application deployed across multiple subdomains, e.g. "heroku"-style platform as a service. Version 3.1.0 of the fastify-csrf fixes it. the vulnerability. The user of the module would need to supply a `userInfo` when generating the CSRF token to fully implement the protection on their end. This is needed only for applications hosted on different subdomains. **CVE ID : CVE-2021-29624**	https://github.com/fastify/csrf/pull/2, https://github.com/fastify/fastify-csrf/security/advisories/GHSA-rc4q-9m69-gqp8, https://github.com/fastify/fastify-csrf/pull/51	A-FAS-FAST-040621/71
feehi					
feehi_cms					
Server-Side Request Forgery (SSRF)	24-May-21	6.4	Feehi CMS 2.1.1 is affected by a Server-side request forgery (SSRF) vulnerability. When the user modifies the HTTP Referer header to any url, the server can make a request to it. **CVE ID : CVE-2021-30108**	N/A	A-FEE-FEEH-040621/72
flask-security_project					
flask-security					
URL Redirection to Untrusted Site ('Open Redirect')	17-May-21	5.8	The Python "Flask-Security-Too" package is used for adding security features to your Flask application. It is an is an independently maintained version of Flask-	https://github.com/Flask-Middleware/flask-security/security/adviso	A-FLA-FLAS-040621/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Security based on the 3.0.0 version of Flask-Security. All versions of Flask-Security-Too allow redirects after many successful views (e.g. /login) by honoring the ?next query param. There is code in FS to validate that the url specified in the next parameter is either relative OR has the same netloc (network location) as the requesting URL. This check utilizes Pythons urlsplit library. However many browsers are very lenient on the kind of URL they accept and 'fill in the blanks' when presented with a possibly incomplete URL. As a concrete example - setting http://login?next=\\\github.com will pass FS's relative URL check however many browsers will gladly convert this to http://github.com. Thus an attacker could send such a link to an unwitting user, using a legitimate site and have it redirect to whatever site they want. This is considered a low severity due to the fact that if Werkzeug is used (which is very common with Flask applications) as the WSGI layer, it by default ALWAYS ensures that the Location header is absolute - thus making this attack vector mute. It is possible for application writers to modify	ries/GHSA-6qmf-fj6m-686c	

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
			this default behavior by setting the 'autocorrect_location_header=False`. **CVE ID : CVE-2021-32618**		
Foxitsoftware					
phantompdf					
Out-of-bounds Write	21-May-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the browseForDoc function. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13523. **CVE ID : CVE-2021-31473**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-040621/74
reader					
Out-of-bounds Write	21-May-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-READ-040621/75

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
			browseForDoc function. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13523. **CVE ID : CVE-2021-31473**		
givewp					
give					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	3.5	The GiveWP â€“ Donation Plugin and Fundraising Platform WordPress plugin before 2.10.4 did not sanitise or escape the Background Image field of its Stripe Checkout Setting and Logo field in its Email settings, leading to authenticated (admin+) Stored XSS issues. **CVE ID : CVE-2021-24315**	https://wpscan.com/vulnerability/006b37c9-641c-4676-a315-9b6053e001d2	A-GIV-GIVE-040621/76
Glpi-project					
glpi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-May-21	4.3	GLPi 9.5.4 does not sanitize the metadata. This way its possible to insert XSS into plugins to execute JavaScript code. **CVE ID : CVE-2021-3486**	N/A	A-GLP-GLPI-040621/77
Gnome					
gupnp					
N/A	24-May-21	5.8	An issue was discovered in GUPnP before 1.0.7 and 1.1.x	https://gitlab.gnome.org	A-GNO-GUPN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 1.2.x before 1.2.5. It allows DNS rebinding. A remote web server can exploit this vulnerability to trick a victim's browser into triggering actions against local UPnP services implemented using this library. Depending on the affected service, this could be used for data exfiltration, data tempering, etc. **CVE ID : CVE-2021-33516**	/GNOME/gupnp/-/issues/24, https://discourse.gnome.org/t/security-relevant-releases-for-gupnp-issue-cve-2021-33516/6536	040621/78
GNU					
glibc					
Use After Free	25-May-21	7.5	The mq_notify function in the GNU C Library (aka glibc) through 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or possibly unspecified other impact. **CVE ID : CVE-2021-33574**	N/A	A-GNU-GLIB-040621/79
gowebsolutions					
wp_customer_reviews					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	3.5	The WP Customer Reviews WordPress plugin before 3.5.6 did not sanitise some of its settings, allowing high privilege users such as administrators to set XSS payloads in them which will then be triggered in pages	https://wpscan.com/vulnerability/c450f54a-3372-49b2-8ad8-68d5cc0dd49e	A-GOW-WP_C-040621/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where reviews are enabled **CVE ID : CVE-2021-24296**		
gris_cms_project					
gris_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	4.3	An issue was discovered in Gris CMS v0.1. There is a Persistent XSS vulnerability which allows remote attackers to inject arbitrary web script or HTML via admin/dashboard. **CVE ID : CVE-2021-30082**	N/A	A-GRI-GRIS-040621/81
hedgedoc					
hedgedoc					
Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	19-May-21	4.3	HedgeDoc is a platform to write and share markdown. HedgeDoc before version 1.8.2 is vulnerable to a cross-site scripting attack using the YAML-metadata of a note. An attacker with write access to a note can embed HTML tags in the Open Graph metadata section of the note, resulting in the frontend rendering the script tag as part of the `<head>` section. Unless your instance prevents guests from editing notes, this vulnerability allows unauthenticated attackers to inject JavaScript into notes that allow guest edits. If your instance prevents guests from editing notes, this vulnerability allows authenticated attackers to inject JavaScript into any note pages they have write-access	https://github.com/hedgedoc/hedgedoc/commit/01dad5821ee28377ebe640c6c72c3e0bb0d51ea7, https://github.com/hedgedoc/hedgedoc/security/advisories/GHSA-gjg7-4j2h-94fq	A-HED-HEDG-040621/82

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
			to. This vulnerability is patched in version 1.8.2. As a workaround, one can disable guest edits until the next update. **CVE ID : CVE-2021-29503**		
Huawei					
manageone					
Insufficient Verification of Data Authenticity	20-May-21	3.5	There is a denial of service vulnerability in some versions of ManageOne. In specific scenarios, due to the insufficient verification of the parameter, an attacker may craft some specific parameter. Successful exploit may cause some services abnormal. **CVE ID : CVE-2021-22339**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-01-dos-en	A-HUA-MANA-040621/83
Improper Handling of Exceptional Conditions	20-May-21	3.5	There is a denial of service vulnerability in some versions of ManageOne. There is a logic error in the implementation of a function of a module. When the service pressure is heavy, there is a low probability that an exception may occur. Successful exploit may cause some services abnormal. **CVE ID : CVE-2021-22409**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-02-dos-en	A-HUA-MANA-040621/84
hyperkitty_project					
hyperkitty					
Exposure of Sensitive Information to an Unauthorized Actor	26-May-21	5	An issue was discovered in management/commands/hyperkitty_import.py in HyperKitty through 1.3.4. When importing a private mailing list's archives, these archives are publicly visible	https://gitlab.com/mailman/hyperkitty/-/issues/380, https://gitlab.com/mailm	A-HYP-HYPE-040621/85

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
			for the duration of the import. For example, sensitive information might be available on the web for an hour during a large migration from Mailman 2 to Mailman 3. **CVE ID : CVE-2021-33038**	an/hyperkitty/-/commit/9025324597d60b2dff740e49b70b15589d6804fa	
ibenic					
simple_giveaways					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	4.3	The method and share GET parameters of the Giveaway pages were not sanitised, validated or escaped before being output back in the pages, thus leading to reflected XSS **CVE ID : CVE-2021-24298**	https://wpscan.com/vulnerability/30aebded-3eb3-4dda-90b5-12de5e622c91	A-IBE-SIMP-040621/86
IBM					
control_center					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-21	3.5	IBM Control Center 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 198761. **CVE ID : CVE-2021-20528**	https://exchange.xforce.ibmcloud.com/vulnerabilities/198761, https://www.ibm.com/support/pages/node/6454215	A-IBM-CONT-040621/87
Exposure of Sensitive Information to an Unauthorized Actor	19-May-21	5	IBM Control Center 6.2.0.0 could allow a user to obtain sensitive version information that could be used in further attacks against the system. IBM X-Force ID: 198763.	https://exchange.xforce.ibmcloud.com/vulnerabilities/198763, https://www.ibm.com/s	A-IBM-CONT-040621/88

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20529	upport/pages/node/6454209	
infosphere_information_server					
Exposure of Sensitive Information to an Unauthorized Actor	21-May-21	5	IBM InfoSphere Information Server 11.7 could allow an attacker to obtain sensitive information by injecting parameters into an HTML query. This information could be used in further attacks against the system. IBM X-Force ID: 199918. **CVE ID : CVE-2021-29681**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199917, https://www.ibm.com/support/pages/node/6454591	A-IBM-INFO-040621/89
Improper Authentication	17-May-21	5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain highly sensitive information due to a vulnerability in the authentication mechanism. IBM X-Force ID: 201775. **CVE ID : CVE-2021-29747**	https://www.ibm.com/support/pages/node/6453437, https://exchange.xforce.ibmcloud.com/vulnerabilities/201775	A-IBM-INFO-040621/90
maximo_asset_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-21	3.5	IBM Maximo Asset Management 7.6.0 and 7.6.1 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195522. **CVE ID : CVE-2021-20374**	https://www.ibm.com/support/pages/node/6454205, https://exchange.xforce.ibmcloud.com/vulnerabilities/195522	A-IBM-MAXI-040621/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
security_guardium					
N/A	24-May-21	9	IBM Security Guardium 11.2 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 195766. **CVE ID : CVE-2021-20385**	https://www.ibm.com/support/pages/node/6455281, https://exchange.xforce.ibmcloud.com/vulnerabilities/195766	A-IBM-SECU-040621/92
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	4.3	IBM Security Guardium 11.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 195767. **CVE ID : CVE-2021-20386**	https://www.ibm.com/support/pages/node/6455281, https://exchange.xforce.ibmcloud.com/vulnerabilities/195767	A-IBM-SECU-040621/93
Insufficiently Protected Credentials	24-May-21	2.1	IBM Security Guardium 11.2 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 195770. **CVE ID : CVE-2021-20389**	https://www.ibm.com/support/pages/node/6455281, https://exchange.xforce.ibmcloud.com/vulnerabilities/195770	A-IBM-SECU-040621/94
Use of a Broken or Risky Cryptographi	24-May-21	5	IBM Security Guardium 11.2 uses weaker than expected cryptographic algorithms that could allow an attacker to	https://www.ibm.com/support/pages/node/6455	A-IBM-SECU-040621/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c Algorithm			decrypt highly sensitive information. IBM X-Force ID: 196280. **CVE ID : CVE-2021-20419**	281, https://exchange.xforce.ibmcloud.com/vulnerabilities/196280	
Use of Hard-coded Credentials	24-May-21	7.5	IBM Security Guardium 11.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 196313. **CVE ID : CVE-2021-20426**	https://www.ibm.com/support/pages/node/6455281, https://exchange.xforce.ibmcloud.com/vulnerabilities/196313	A-IBM-SECU-040621/96
Generation of Error Message Containing Sensitive Information	24-May-21	5	IBM Security Guardium 11.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196315. **CVE ID : CVE-2021-20428**	https://www.ibm.com/support/pages/node/6455281, https://exchange.xforce.ibmcloud.com/vulnerabilities/196315	A-IBM-SECU-040621/97
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-May-21	9	IBM Security Guardium 11.2 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 199184. **CVE ID : CVE-2021-20557**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199184, https://www.ibm.com/support/pages/node/6455269	A-IBM-SECU-040621/98
security_identity_manager					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 199997 **CVE ID : CVE-2021-29682**	https://www.ibm.com/support/pages/node/6454587, https://exchange.xforce.ibmcloud.com/vulnerabilities/199997	A-IBM-SECU-040621/99
Cleartext Storage of Sensitive Information	20-May-21	4	IBM Security Identity Manager 7.0.2 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 199998. **CVE ID : CVE-2021-29683**	https://www.ibm.com/support/pages/node/6454587, https://exchange.xforce.ibmcloud.com/vulnerabilities/199998	A-IBM-SECU-040621/100
Incorrect Permission Assignment for Critical Resource	20-May-21	6.5	IBM Security Identity Manager 7.0.2 could allow an authenticated user to bypass security and perform actions that they should not have access to. IBM X-Force ID: 200015 **CVE ID : CVE-2021-29686**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200015, https://www.ibm.com/support/pages/node/6454587	A-IBM-SECU-040621/101
Observable Discrepancy	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote user to enumerate usernames due to a difference of responses from valid and invalid login attempts. IBM X-Force ID: 200018 **CVE ID : CVE-2021-29687**	https://www.ibm.com/support/pages/node/6454605, https://exchange.xforce.ibmcloud.com/vulnerabiliti	A-IBM-SECU-040621/102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				es/200018	
Generation of Error Message Containing Sensitive Information	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 200102. **CVE ID : CVE-2021-29688**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200102, https://www.ibm.com/support/pages/node/6454605, https://www.ibm.com/support/pages/node/6454587	A-IBM-SECU-040621/103
Use of Hard-coded Credentials	20-May-21	5	IBM Security Identity Manager 7.0.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 200252. **CVE ID : CVE-2021-29691**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200252, https://www.ibm.com/support/pages/node/6454587	A-IBM-SECU-040621/104
N/A	20-May-21	4.3	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 200253.	https://exchange.xforce.ibmcloud.com/vulnerabilities/200253, https://www.ibm.com/support/pages/node/6454587	A-IBM-SECU-040621/105

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
			CVE ID : CVE-2021-29692		
spectrum_scale					
Improper Privilege Management	25-May-21	4.6	IBM Spectrum Scale 5.1.0.1 could allow a local with access to the GUI pod container to obtain sensitive cryptographic keys that could allow them to elevate their privileges. IBM X-Force ID: 200883. **CVE ID : CVE-2021-29708**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200883, https://www.ibm.com/support/pages/node/6455629	A-IBM-SPEC-040621/106
invoiceplane					
invoiceplane					
Improper Restriction of Excessive Authentication Attempts	17-May-21	5	InvoicePlane 1.5.11 doesn't have any rate-limiting for password reset and the reset token is generated using a weak mechanism that is predictable. **CVE ID : CVE-2021-29023**	N/A	A-INV-INVO-040621/107
Files or Directories Accessible to External Parties	17-May-21	5	In InvoicePlane 1.5.11 a misconfigured web server allows unauthenticated directory listing and file download. Allowing an attacker to directory traversal and download files suppose to be private without authentication. **CVE ID : CVE-2021-29024**	N/A	A-INV-INVO-040621/108
Jenkins					
filesystem_trigger					
Improper Restriction of XML External Entity	25-May-21	6.5	Jenkins Filesystem Trigger Plugin 0.40 and earlier does not configure its XML parser to prevent XML external entity	https://www.jenkins.io/security/advisory/2021-05-	A-JEN-FILE-040621/109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reference			(XXE) attacks. **CVE ID : CVE-2021-21657**	25/#SECURITY-2339	
markdown_formatter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-May-21	3.5	Jenkins Markdown Formatter Plugin 0.1.0 and earlier does not sanitize crafted link target URLs, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with the ability to edit any description rendered using the configured markup formatter. **CVE ID : CVE-2021-21660**	https://www.jenkins.io/security/advisory/2021-05-25/#SECURITY-2198	A-JEN-MARK-040621/110
nuget					
Improper Restriction of XML External Entity Reference	25-May-21	6.4	Jenkins Nuget Plugin 1.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2021-21658**	https://www.jenkins.io/security/advisory/2021-05-25/#SECURITY-2340	A-JEN-NUGE-040621/111
urltrigger					
Improper Restriction of XML External Entity Reference	25-May-21	5.5	Jenkins URLTrigger Plugin 0.48 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2021-21659**	https://www.jenkins.io/security/advisory/2021-05-25/#SECURITY-2341	A-JEN-URLT-040621/112
Joomla					
joomla\\!					
Improper Neutralization of Input During Web Page Generation	26-May-21	4.3	An issue was discovered in Joomla! 3.0.0 through 3.9.26. HTML was missing in the executable block list of MediaHelper::canUpload,	https://developer.joomla.org/security-centre/852-20210501-core-adding-	A-JOO-JOOM-040621/113

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')			leading to XSS attack vectors. **CVE ID : CVE-2021-26032**	html-to-the-executable-block-list-of-mediahelper-canupload.html	
Cross-Site Request Forgery (CSRF)	26-May-21	4.3	An issue was discovered in Joomla! 3.0.0 through 3.9.26. A missing token check causes a CSRF vulnerability in the AJAX reordering endpoint. **CVE ID : CVE-2021-26033**	https://developer.joomla.org/security-centre/853-20210502-core-csrf-in-ajax-reordering-endpoint.html	A-JOO-JOOM-040621/114
Cross-Site Request Forgery (CSRF)	26-May-21	4.3	An issue was discovered in Joomla! 3.0.0 through 3.9.26. A missing token check causes a CSRF vulnerability in data download endpoints in com_banners and com_sysinfo. **CVE ID : CVE-2021-26034**	https://developer.joomla.org/security-centre/854-20210503-core-csrf-in-data-download-endpoints.html	A-JOO-JOOM-040621/115
keystonejs					
keystone-5					
Exposure of Sensitive Information to an Unauthorized Actor	24-May-21	3.5	Keystone 5 is an open source CMS platform to build Node.js applications. This security advisory relates to a newly discovered capability in our query infrastructure to directly or indirectly expose the values of private fields, bypassing the configured access control. This is an access control related oracle attack in that the attack	https://github.com/keystonejs/keystone-5/security/advisories/GHSA-27g8-r9vw-765x	A-KEY-KEYS-040621/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			method guides an attacker during their attempt to reveal information they do not have access to. The complexity of completing the attack is limited by some length-dependent behaviors and the fidelity of the exposed information. Under some circumstances, field values or field value meta data can be determined, despite the field or list having `read` access control configured. If you use private fields or lists, you may be impacted. No patches exist at this time. There are no workarounds at this time **CVE ID : CVE-2021-32624**		
koa-remove-trailing-slashes_project					
koa-remove-trailing-slashes					
URL Redirection to Untrusted Site ('Open Redirect')	17-May-21	5.8	The package koa-remove-trailing-slashes before 2.0.2 are vulnerable to Open Redirect via the use of trailing double slashes in the URL when accessing the vulnerable endpoint (such as https://example.com//attacker.example/). The vulnerable code is in index.js::removeTrailingSlashes(), as the web server uses relative URLs instead of absolute URLs. **CVE ID : CVE-2021-23384**	N/A	A-KOA-KOA--040621/117
kujirahand					
konawiki					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-May-21	7.5	SQL injection vulnerability in the KonaWiki2 versions prior to 2.2.4 allows remote attackers to execute arbitrary SQL commands and to obtain/alter the information stored in the database via unspecified vectors. **CVE ID : CVE-2021-20720**	https://kujirahand.com/konawiki/	A-KUJ-KONA-040621/118
Unrestricted Upload of File with Dangerous Type	20-May-21	7.5	KonaWiki2 versions prior to 2.2.4 allows a remote attacker to upload arbitrary files via unspecified vectors. If the file contains PHP scripts, arbitrary code may be executed. **CVE ID : CVE-2021-20721**	https://kujirahand.com/konawiki/	A-KUJ-KONA-040621/119
libcaca_project					
libcaca					
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-May-21	7.5	A flaw was found in libcaca. A heap buffer overflow in export.c in function export_tga might lead to memory corruption and other potential consequences. **CVE ID : CVE-2021-30498**	N/A	A-LIB-LIBC-040621/120
Liferay					
dxp					
Generation of Error Message Containing Sensitive Information	16-May-21	5	The JSON web services in Liferay Portal 7.3.4 and earlier, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 20 and 7.2 before fix pack 10 may provide overly verbose error messages, which allows remote attackers to use the contents	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/co	A-LIF-DXP-040621/121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of error messages to help launch another, more focused attacks via crafted inputs. **CVE ID : CVE-2021-29040**	ntent/id/120743429, http://liferay.com	
N/A	16-May-21	4	Denial-of-service (DoS) vulnerability in the Multi-Factor Authentication module in Liferay DXP 7.3 before fix pack 1 allows remote authenticated attackers to prevent any user from authenticating by (1) enabling Time-based One-time password (TOTP) on behalf of the other user or (2) modifying the other user's TOTP shared secret. **CVE ID : CVE-2021-29041**	https://issues.liferay.com/browse/LPE-17131, http://liferay.com	A-LIF-DXP-040621/122
Exposure of Sensitive Information to an Unauthorized Actor	17-May-21	4.3	The Portal Store module in Liferay Portal 7.0.0 through 7.3.5, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pack 1 does not obfuscate the S3 store's proxy password, which allows attackers to steal the proxy password via man-in-the-middle attacks or shoulder surfing. **CVE ID : CVE-2021-29043**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743515, http://liferay.com	A-LIF-DXP-040621/123
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Site module's membership request administration pages in Liferay Portal 7.0.0 through 7.3.5, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 21, 7.2 before fix pack	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mx	A-LIF-DXP-040621/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10 and 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_site_my_sites_web_portlet_MySitesPortlet_comments parameter. **CVE ID : CVE-2021-29044**	mVrnXW/content/id/120743548, http://liferay.com	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Redirect module's redirection administration page in Liferay Portal 7.3.2 through 7.3.5, and Liferay DXP 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_redirect_web_internal_portlet_RedirectPortlet_destinationURL parameter. **CVE ID : CVE-2021-29045**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743484	A-LIF-DXP-040621/125
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Asset module's category selector input field in Liferay Portal 7.3.5 and Liferay DXP 7.3 before fix pack 1, allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_asset_categories_admin_web_portlet_AssetCategoriesAdminPortlet_title parameter. **CVE ID : CVE-2021-29046**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743501	A-LIF-DXP-040621/126
Improper Authentication	16-May-21	5	The SimpleCaptcha implementation in Liferay Portal 7.3.4, 7.3.5 and Liferay DXP 7.3 before fix pack 1 does	https://portal.liferay.dev/learn/security/known-	A-LIF-DXP-040621/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not invalidate CAPTCHA answers after it is used, which allows remote attackers to repeatedly perform actions protected by a CAPTCHA challenge by reusing the same CAPTCHA answer. **CVE ID : CVE-2021-29047**	vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743467, http://liferay.com	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Layout module's page administration page in Liferay Portal 7.3.4, 7.3.5 and Liferay DXP 7.2 before fix pack 11 and 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_layout_admin_web_portlet_GroupPagesPortlet_name parameter. **CVE ID : CVE-2021-29048**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743601	A-LIF-DXP-040621/128
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Asset module's Asset Publisher app in Liferay Portal 7.2.1 through 7.3.5, and Liferay DXP 7.1 before fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_XXXXXXXXXXXX_assetEntryId parameter. **CVE ID : CVE-2021-29051**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743580	A-LIF-DXP-040621/129
Incorrect Default	17-May-21	4	The Data Engine module in Liferay Portal 7.3.0 through	https://portal.liferay.dev	A-LIF-DXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			7.3.5, and Liferay DXP 7.3 before fix pack 1 does not check permissions in DataDefinitionResourceImpl.getSiteDataDefinitionByContentTypeByDataDefinitionKey, which allows remote authenticated users to view DDMStructures via GET API calls. **CVE ID : CVE-2021-29052**	/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743159, http://liferay.com	040621/130
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-21	6.5	Multiple SQL injection vulnerabilities in Liferay Portal 7.3.5 and Liferay DXP 7.3 before fix pack 1 allow remote authenticated users to execute arbitrary SQL commands via the classPKField parameter to (1) CommerceChannelRelFinder.countByC_C, or (2) CommerceChannelRelFinder.findByC_C. **CVE ID : CVE-2021-29053**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120778225	A-LIF-DXP-040621/131
liferay_portal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Asset module's categories administration page in Liferay Portal 7.3.4 allows remote attackers to inject arbitrary web script or HTML via the site name. **CVE ID : CVE-2021-29039**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120777766, http://liferay.com	A-LIF-LIFE-040621/132
Generation	16-May-21	5	The JSON web services in	https://port	A-LIF-LIFE-

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
of Error Message Containing Sensitive Information			Liferay Portal 7.3.4 and earlier, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 20 and 7.2 before fix pack 10 may provide overly verbose error messages, which allows remote attackers to use the contents of error messages to help launch another, more focused attacks via crafted inputs. **CVE ID : CVE-2021-29040**	al.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743429, http://liferay.com	040621/133
Exposure of Sensitive Information to an Unauthorized Actor	17-May-21	4.3	The Portal Store module in Liferay Portal 7.0.0 through 7.3.5, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pack 1 does not obfuscate the S3 store's proxy password, which allows attackers to steal the proxy password via man-in-the-middle attacks or shoulder surfing. **CVE ID : CVE-2021-29043**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743515, http://liferay.com	A-LIF-LIFE-040621/134
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Site module's membership request administration pages in Liferay Portal 7.0.0 through 7.3.5, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_site_my_sites_web_portlet_MySitesPortlet_comments parameter.	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743548, http://liferay.com	A-LIF-LIFE-040621/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29044		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Redirect module's redirection administration page in Liferay Portal 7.3.2 through 7.3.5, and Liferay DXP 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_redirect_web_internal_portlet_RedirectPortlet_destinationURL parameter. **CVE ID : CVE-2021-29045**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743484	A-LIF-LIFE-040621/136
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Asset module's category selector input field in Liferay Portal 7.3.5 and Liferay DXP 7.3 before fix pack 1, allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_asset_categories_admin_web_portlet_AssetCategoriesAdminPortlet_title parameter. **CVE ID : CVE-2021-29046**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743501	A-LIF-LIFE-040621/137
Improper Authentication	16-May-21	5	The SimpleCaptcha implementation in Liferay Portal 7.3.4, 7.3.5 and Liferay DXP 7.3 before fix pack 1 does not invalidate CAPTCHA answers after it is used, which allows remote attackers to repeatedly perform actions protected by a CAPTCHA challenge by reusing the same CAPTCHA answer.	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743467, http://lifera	A-LIF-LIFE-040621/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29047	y.com	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Layout module's page administration page in Liferay Portal 7.3.4, 7.3.5 and Liferay DXP 7.2 before fix pack 11 and 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_layout_admin_web_portlet_GroupPagesPortlet_name parameter. **CVE ID : CVE-2021-29048**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743601	A-LIF-LIFE-040621/139
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	Cross-site scripting (XSS) vulnerability in the Asset module's Asset Publisher app in Liferay Portal 7.2.1 through 7.3.5, and Liferay DXP 7.1 before fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_XXXXXXXXXXXX_assetEntryId parameter. **CVE ID : CVE-2021-29051**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120743580	A-LIF-LIFE-040621/140
Incorrect Default Permissions	17-May-21	4	The Data Engine module in Liferay Portal 7.3.0 through 7.3.5, and Liferay DXP 7.3 before fix pack 1 does not check permissions in DataDefinitionResourceImpl.getSiteDataDefinitionByContentTypeByDataDefinitionKey, which allows remote authenticated users to view	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120	A-LIF-LIFE-040621/141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DDMStructures via GET API calls. **CVE ID : CVE-2021-29052**	743159, http://liferay.com	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-21	6.5	Multiple SQL injection vulnerabilities in Liferay Portal 7.3.5 and Liferay DXP 7.3 before fix pack 1 allow remote authenticated users to execute arbitrary SQL commands via the classPKField parameter to (1) CommerceChannelRelFinder.countByC_C, or (2) CommerceChannelRelFinder.findByC_C. **CVE ID : CVE-2021-29053**	http://liferay.com, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120778225	A-LIF-LIFE-040621/142
lifterlms					
lifterlms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	3.5	The 'State' field of the Edit profile page of the LMS by LifterLMS – Online Course, Membership & Learning Management System Plugin for WordPress plugin before 4.21.1 is not properly sanitised when output in the About section of the profile page, leading to a stored Cross-Site Scripting issue. This could allow low privilege users (such as students) to elevate their privilege via an XSS attack when an admin will view their profile. **CVE ID : CVE-2021-24308**	https://wpscan.com/vulnerability/f29f68a5-6575-441d-98c9-867145f2b082	A-LIF-LIFT-040621/143
linaro					
trusted_firmware-m					
Missing	21-May-21	5	In Trusted Firmware-M	https://git.tr	A-LIN-TRUS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release of Memory after Effective Lifetime			through 1.3.0, cleaning up the memory allocated for a multi-part cryptographic operation (in the event of a failure) can prevent the abort() operation in the associated cryptographic library from freeing internal resources, causing a memory leak. **CVE ID : CVE-2021-32032**	ustedfirmware.org/TF-M/trusted-firmware-m.git/tree/docs/security/security_advisories/crypto_multi_part_ops_abort_fail.rst, https://www.trustedfirmware.org	040621/144
lucyparsonslabs					
openoversight					
Cross-Site Request Forgery (CSRF)	25-May-21	5.8	Cross-site request forgery in OpenOversight 0.6.4 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link. **CVE ID : CVE-2021-20096**	N/A	A-LUC-OPEN-040621/145
mailform01_project					
mailform01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	4.3	Reflected cross-site scripting vulnerability in [MailForm01] free edition (versions which the last updated date listed at the top of descriptions in the program file is from 2014 December 12 to 2018 July 27) allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20723**	N/A	A-MAI-MAIL-040621/146
malwarefox					
antimalware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	17-May-21	7.2	Incorrect access control in zam64.sys, zam32.sys in MalwareFox AntiMalware 2.74.0.150 where IOCTL's 0x80002014, 0x80002018 expose unrestricted disk read/write capabilities respectively. A non-privileged process can open a handle to \.\ZemanaAntiMalware, register with the driver using IOCTL 0x80002010 and send these IOCTL's to escalate privileges by overwriting the boot sector or overwriting critical code in the pagefile. **CVE ID : CVE-2021-31727**	N/A	A-MAL-ANTI-040621/147
Incorrect Authorization	17-May-21	7.2	Incorrect access control in zam64.sys, zam32.sys in MalwareFox AntiMalware 2.74.0.150 allows a non-privileged process to open a handle to \.\ZemanaAntiMalware, register itself with the driver by sending IOCTL 0x80002010, allocate executable memory using a flaw in IOCTL 0x80002040, install a hook with IOCTL 0x80002044 and execute the executable memory using this hook with IOCTL 0x80002014 or 0x80002018, this exposes ring 0 code execution in the context of the driver allowing the non-privileged process to elevate privileges. **CVE ID : CVE-2021-31728**	N/A	A-MAL-ANTI-040621/148
matrix-react-sdk_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
matrix-react-sdk					
Unrestricted Upload of File with Dangerous Type	17-May-21	4.4	Matrix-React-SDK is a react-based SDK for inserting a Matrix chat/voip client into a web page. Before version 3.21.0, when uploading a file, the local file preview can lead to execution of scripts embedded in the uploaded file. This can only occur after several user interactions to open the preview in a separate tab. This only impacts the local user while in the process of uploading. It cannot be exploited remotely or by other users. This vulnerability is patched in version 3.21.0. **CVE ID : CVE-2021-32622**	https://github.com/matrix-org/matrix-react-sdk/pull/5981, https://github.com/matrix-org/matrix-react-sdk/security/advisories/GHSA-8796-gc9j-63rv	A-MAT-MATR-040621/149
mediateknet					
netwave_system					
Exposure of Sensitive Information to an Unauthorized Actor	25-May-21	5	An information disclosure vulnerability was discovered in /index.class.php (via port 8181) on NetWave System 1.0 which allows unauthenticated attackers to exfiltrate sensitive information from the system. **CVE ID : CVE-2021-27823**	https://www.mediateknet.net/	A-MED-NETW-040621/150
Microsoft					
.net					
Exposure of Sensitive Information to an Unauthorize	20-May-21	5	Products with Unified Automation .NET based OPC UA Client/Server SDK Bundle: Versions V3.0.7 and prior (.NET 4.5, 4.0, and 3.5	N/A	A-MIC-.NET-040621/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Actor			Framework versions only) are vulnerable to an uncontrolled recursion, which may allow an attacker to trigger a stack overflow. **CVE ID : CVE-2021-27434**		
mlfactory					
dsgvo_all_in_one_for_wp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	4.3	The dsgvoaio_write_log AJAX action of the DSGVO All in one for WP WordPress plugin before 4.0 did not sanitise or escape some POST parameter submitted before outputting them in the Log page in the administrator dashboard (wp-admin/admin.php?page=dsgvoaiofree-show-log). This could allow unauthenticated attackers to gain unauthorised access by using an XSS payload to create a rogue administrator account, which will be trigged when an administrator will view the logs. **CVE ID : CVE-2021-24294**	https://wpscan.com/vulnerability/43b8cfb4-f875-432b-8e3b-52653fdee87c	A-MLF-DSGV-040621/152
mpv					
mpv					
Use of Externally-Controlled Format String	18-May-21	6.8	A format string vulnerability in mpv through 0.33.0 allows user-assisted remote attackers to achieve code execution via a crafted m3u playlist file. **CVE ID : CVE-2021-30145**	https://mpv.io, https://github.com/mpv-player/mpv/commit/d0c530919d8cd4d7a774e38ab064e0fabd	A-MPV-MPV-040621/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ae34e6	
mrxvt_project					
mrxvt					
Improper Handling of Exceptional Conditions	20-May-21	6.5	rxvt-unicode 9.22, rxvt 2.7.10, mrxvt 0.5.4, and Eterm 0.9.7 allow (potentially remote) code execution because of improper handling of certain escape sequences (ESC G Q). A response is terminated by a newline. **CVE ID : CVE-2021-33477**	http://cvs.schmorp.de/rxvt-unicode/src/command.C?r1=1.582&r2=1.583	A-MRX-MRXV-040621/154
nconf-toml_project					
nconf-toml					
N/A	25-May-21	7.5	Prototype pollution vulnerability in `nconf-toml` versions 0.0.1 through 0.0.2 allows an attacker to cause a denial of service and may lead to remote code execution. **CVE ID : CVE-2021-25946**	N/A	A-NCO-NCON-040621/155
neox					
hana_flv_player					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	3.5	The Hana Flv Player WordPress plugin through 3.1.3 is vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) vulnerability within the 'Default Skin' field. **CVE ID : CVE-2021-24302**	https://wpscan.com/vulnerability/372a66ca-1c3c-4429-86a5-81dbdaa9ec7d	A-NEO-HANA-040621/156
normalize-url_project					
normalize-url					
N/A	24-May-21	5	The normalize-url package before 4.5.1, 5.x before 5.3.1, and 6.x before 6.0.1 for	https://github.com/sindresorhus/nor	A-NOR-NORM-040621/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Node.js has a ReDoS (regular expression denial of service) issue because it has exponential performance for data: URLs. **CVE ID : CVE-2021-33502**	malize-url/releases/tag/v6.0.1	
NSA					
emissary					
Deserialization of Untrusted Data	21-May-21	6.5	Emissary is a distributed, peer-to-peer, data-driven workflow framework. Emissary 6.4.0 is vulnerable to Unsafe Deserialization of post-authenticated requests to the [`WorkSpaceClientEnqueue.action`](https://github.com/NationalSecurityAgency/emissary/blob/30c54ef16c6eb6ed09604a929939fb9f66868382/src/main/java/emissary/server/mvc/internal/WorkSpaceClientEnqueueAction.java) REST endpoint. This issue may lead to post-auth Remote Code Execution. This issue has been patched in version 6.5.0. As a workaround, one can disable network access to Emissary from untrusted sources. **CVE ID : CVE-2021-32634**	https://github.com/NationalSecurityAgency/emissary/security/advisories/GHSA-m5qf-gfmp-7638, https://github.com/NationalSecurityAgency/emissary/commit/40260b1ec1f76cc92361702cc14fa1e4388e19d7	A-NSA-EMIS-040621/158
opcfoundation					
ua-.net-legacy					
Uncontrolled Recursion	20-May-21	5	OPC Foundation UA .NET Standard versions prior to 1.4.365.48 and OPC UA .NET Legacy are vulnerable to an uncontrolled recursion, which may allow an attacker to	N/A	A-OPC-UA-.-040621/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			trigger a stack overflow. **CVE ID : CVE-2021-27432**		
ua_.net_standard_stack					
Uncontrolled Recursion	20-May-21	5	OPC Foundation UA .NET Standard versions prior to 1.4.365.48 and OPC UA .NET Legacy are vulnerable to an uncontrolled recursion, which may allow an attacker to trigger a stack overflow. **CVE ID : CVE-2021-27432**	N/A	A-OPC-UA_.-040621/160
Opennms					
horizon					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	3.5	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-Site Scripting since there is no validation on the input being sent to the `name` parameter in `noticeWizard` endpoint. Due to this flaw an authenticated attacker could inject arbitrary script and trick other admin users into downloading malicious files. **CVE ID : CVE-2021-25929**	https://github.com/OpenNMS/opennms/commit/eb08b5ed4c5548f3e941a1f0d0363ae4439fa98c, https://github.com/OpenNMS/opennms/commit/66c1f626bf38a7d1a9530b4d68598269ee5245a2	A-OPE-HORI-040621/161
Cross-Site Request Forgery (CSRF)	20-May-21	4.3	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions	https://github.com/OpenNMS/opennms/commit/	A-OPE-HORI-040621/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to CSRF, due to no CSRF protection, and since there is no validation of an existing user name while renaming a user. As a result, privileges of the renamed user are being overwritten by the old user and the old user is being deleted from the user list. **CVE ID : CVE-2021-25930**	607151ea8f90212a3fb37c977fa57c7d58d26a84, https://github.com/OpenNMS/opennms/commit/eb08b5ed4c5548f3e941a1f0d0363ae4439fa98c	
Cross-Site Request Forgery (CSRF)	20-May-21	6.8	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to CSRF, due to no CSRF protection at `/opennms/admin/userGroupView/users/updateUser`. This flaw allows assigning `ROLE_ADMIN` security role to a normal user. Using this flaw, an attacker can trick the admin user to assign administrator privileges to a normal user by enticing him to click upon an attacker-controlled website.	https://github.com/OpenNMS/opennms/commit/607151ea8f90212a3fb37c977fa57c7d58d26a84, https://github.com/OpenNMS/opennms/commit/eb08b5ed4c5548f3e941a1f0d0363ae4439fa98c	A-OPE-HORI-040621/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-25931		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	3.5	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-Site Scripting, since the function `validateFormInput()` performs improper validation checks on the input sent to the `groupName` and `groupComment` parameters. Due to this flaw, an authenticated attacker could inject arbitrary script and trick other admin users into downloading malicious files which can cause severe damage to the organization using opennms. **CVE ID : CVE-2021-25933**	https://github.com/OpenNMS/opennms/commit/f3ebfa3da5352b4d57f238b54c6db315ad99f10e, https://github.com/OpenNMS/opennms/commit/eb08b5ed4c5548f3e941a1f0d0363ae4439fa98c, https://github.com/OpenNMS/opennms/commit/8a97e6869d6e49da18b208c837438ace80049c01,	A-OPE-HORI-040621/164
meridian					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	3.5	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-	https://github.com/OpenNMS/opennms/commit/eb08b5ed4c5548f3e941a1f0d0363ae4439fa98c, https://github.com/OpenNMS/openn	A-OPE-MERI-040621/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Site Scripting since there is no validation on the input being sent to the `name` parameter in `noticeWizard` endpoint. Due to this flaw an authenticated attacker could inject arbitrary script and trick other admin users into downloading malicious files. **CVE ID : CVE-2021-25929**	ms/commit/66c1f626bf38a7d1a9530b4d68598269ee5245a2	
Cross-Site Request Forgery (CSRF)	20-May-21	4.3	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to CSRF, due to no CSRF protection, and since there is no validation of an existing user name while renaming a user. As a result, privileges of the renamed user are being overwritten by the old user and the old user is being deleted from the user list. **CVE ID : CVE-2021-25930**	https://github.com/OpenNMS/opennms/commit/607151ea8f90212a3fb37c977fa57c7d58d26a84, https://github.com/OpenNMS/opennms/commit/eb08b5ed4c5548f3e941a1f0d0363ae4439fa98c	A-OPE-MERI-040621/166
Cross-Site Request Forgery (CSRF)	20-May-21	6.8	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-	https://github.com/OpenNMS/opennms/commit/607151ea8f90212a3fb37c977fa57c7d58d26a84, https://githu	A-OPE-MERI-040621/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			foundation-2020.1.6-1 are vulnerable to CSRF, due to no CSRF protection at `/opennms/admin/userGroupView/users/updateUser`. This flaw allows assigning `ROLE_ADMIN` security role to a normal user. Using this flaw, an attacker can trick the admin user to assign administrator privileges to a normal user by enticing him to click upon an attacker-controlled website. **CVE ID : CVE-2021-25931**	b.com/OpenNMS/opennms/commit/eb08b5ed4c5548f3e941a1f0d0363ae4439fa98c	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	3.5	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-Site Scripting, since the function `validateFormInput()` performs improper validation checks on the input sent to the `groupName` and `groupComment` parameters. Due to this flaw, an authenticated attacker could inject arbitrary script and trick other admin users into downloading malicious files which can cause severe damage to the organization	https://github.com/OpenNMS/opennms/commit/f3ebfa3da5352b4d57f238b54c6db315ad99f10e, https://github.com/OpenNMS/opennms/commit/eb08b5ed4c5548f3e941a1f0d0363ae4439fa98c, https://github.com/OpenNMS/opennms/commit/8a97e6869d6e49da18b208c837438ace80049c01,	A-OPE-MERI-040621/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using opennms. **CVE ID : CVE-2021-25933**		
Opensuse					
libsolv					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-21	4.3	Buffer overflow vulnerability in libsolv 2020-12-13 via the Solver * testcase_read(Pool *pool, FILE *fp, const char *testcase, Queue *job, char **resultp, int *resultflagsp function at src/testcase.c: line 2334, which could cause a denial of service **CVE ID : CVE-2021-3200**	N/A	A-OPE-LIBS-040621/169
overwolf					
overwolf					
Untrusted Search Path	24-May-21	4.4	Untrusted search path vulnerability in The Installer of Overwolf 2.168.0.n and earlier allows an attacker to gain privileges and execute arbitrary code with the privilege of the user invoking the installer via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2021-20726**	https://www.overwolf.com/	A-OVE-OVER-040621/170
Owncloud					
owncloud					
Incorrect Authorization	20-May-21	4	ownCloud 10.7 has an incorrect access control vulnerability, leading to remote information disclosure. Due to a bug in the related API endpoint, the attacker can enumerate all users in a single request by	https://owncloud.com/security-advisories/cve-2021-29659/, https://doc.owncloud.com	A-OWN-OWNC-040621/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			entering three whitespaces. Secondary, the retrieval of all users on a large instance could cause higher than average load on the instance. **CVE ID : CVE-2021-29659**	/server/admin_manual/release_notes.html	
pajbot					
pajbot					
Cross-Site Request Forgery (CSRF)	20-May-21	4.3	Pajbot is a Twitch chat bot. Pajbot versions prior to 1.52 are vulnerable to cross-site request forgery (CSRF). Hosters of the bot should upgrade to `v1.52` or `stable` to install the patch or, as a workaround, can add one modern dependency. **CVE ID : CVE-2021-32632**	https://github.com/pajbot/pajbot/security/advisories/GHSA-wmfr-qrg4-qc3h	A-PAJ-PAJB-040621/172
pgxn					
pg_partman					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-May-21	7.5	In the pg_partman (aka PG Partition Manager) extension before 4.5.1 for PostgreSQL, arbitrary code execution can be achieved via SECURITY DEFINER functions because an explicit search_path is not set. **CVE ID : CVE-2021-33204**	https://github.com/pgpartman/pg_partman/compare/v4.5.0...v4.5.1, https://github.com/pgpartman/pg_partman/commit/0b6565ad378c358f8a6cd1d48ddc482eb7f854d3	A-PGX-PG_P-040621/173
pickplugins					
product_slider_for_woocommerce					
Improper Neutralizatio	24-May-21	4.3	The slider import search feature of the PickPlugins	https://wpscan.com/vuln	A-PIC-PROD-

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
n of Input During Web Page Generation ('Cross-site Scripting')			Product Slider for WooCommerce WordPress plugin before 1.13.22 did not properly sanitised the keyword GET parameter, leading to reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24300**	erability/5fbbc7ad-3f1a-48a1-b2eb-e57f153eb837	040621/174
pixar					
ruby-jss					
N/A	25-May-21	7.5	The Pixar ruby-jss gem before 1.6.0 allows remote attackers to execute arbitrary code because of the Plist gem's documented behavior of using Marshal.load during XML document processing. **CVE ID : CVE-2021-33575**	N/A	A-PIX-RUBY-040621/175
Plone					
plone					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-May-21	6.5	Zope is an open-source web application server. In Zope versions prior to 4.6 and 5.2, users can access untrusted modules indirectly through Python modules that are available for direct use. By default, only users with the Manager role can add or edit Zope Page Templates through the web, but sites that allow untrusted users to add/edit Zope Page Templates through the web are at risk from this vulnerability. The problem has been fixed in Zope 5.2 and 4.6. As a workaround, a site administrator can restrict adding/editing Zope Page	https://github.com/zopefoundation/Zope/commit/1f8456bf1f908ea46012537d52bd7e752a532c91, https://github.com/zopefoundation/Zope/security/advisories/GHSA-5pr9-v234-jw36	A-PLO-PLON-040621/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Templates through the web using the standard Zope user/role permission mechanisms. Untrusted users should not be assigned the Zope Manager role and adding/editing Zope Page Templates through the web should be restricted to trusted users only. **CVE ID : CVE-2021-32633**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	3.5	Plone CMS until version 5.2.4 has a stored Cross-Site Scripting (XSS) vulnerability in the user fullname property and the file upload functionality. The user's input data is not properly encoded when being echoed back to the user. This data can be interpreted as executable code by the browser and allows an attacker to execute JavaScript in the context of the victim's browser if the victim opens a vulnerable page containing an XSS payload. **CVE ID : CVE-2021-3313**	https://plone.org/download/releases/5.2.3, https://plone.org/security/hotfix/20210518	A-PLO-PLON-040621/177
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-May-21	4.3	Zope Products.CMFCore before 2.5.1 and Products.PluggableAuthService before 2.6.2, as used in Plone through 5.2.4 and other products, allow Reflected XSS. **CVE ID : CVE-2021-33507**	https://plone.org/security/hotfix/20210518/reflected-xss-in-various-spots	A-PLO-PLON-040621/178
Improper Neutralization of Input During Web	21-May-21	3.5	Plone through 5.2.4 allows XSS via a full name that is mishandled during rendering of the ownership tab of a	https://plone.org/security/hotfix/20210518/store	A-PLO-PLON-040621/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			content item. **CVE ID : CVE-2021-33508**	d-xss-from-user-fullname	
Incorrect Permission Assignment for Critical Resource	21-May-21	8.5	Plone through 5.2.4 allows remote authenticated managers to perform disk I/O via crafted keyword arguments to the ReStructuredText transform in a Python script. **CVE ID : CVE-2021-33509**	https://plone.org/security/hotfix/20210518/writing-arbitrary-files-via-docutils-and-python-script	A-PLO-PLON-040621/180
Server-Side Request Forgery (SSRF)	21-May-21	4	Plone through 5.2.4 allows remote authenticated managers to conduct SSRF attacks via an event ical URL, to read one line of a file. **CVE ID : CVE-2021-33510**	https://plone.org/security/hotfix/20210518/server-side-request-forgery-via-event-ical-url	A-PLO-PLON-040621/181
Server-Side Request Forgery (SSRF)	21-May-21	5	Plone though 5.2.4 allows SSRF via the lxml parser. This affects Diazo themes, Dexterity TTW schemas, and modeleditors in plone.app.theming, plone.app.dexterity, and plone.supermodel. **CVE ID : CVE-2021-33511**	https://plone.org/security/hotfix/20210518/server-side-request-forgery-via-lxml-parser	A-PLO-PLON-040621/182
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-May-21	3.5	Plone through 5.2.4 allows stored XSS attacks (by a Contributor) by uploading an SVG or HTML document. **CVE ID : CVE-2021-33512**	https://plone.org/security/hotfix/20210518/stored-xss-from-file-upload-svg-html	A-PLO-PLON-040621/183
Improper	21-May-21	3.5	Plone through 5.2.4 allows	https://plon	A-PLO-PLON-

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
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			XSS via the inline_diff methods in Products.CMFDiffTool. **CVE ID : CVE-2021-33513**	e.org/security/hotfix/20210518/xss-vulnerability-in-cmfdifftool	040621/184
postbird_project					
postbird					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-May-21	3.5	Postbird 0.8.4 allows stored XSS via the onerror attribute of an IMG element in any PostgreSQL database table. This can result in reading local files via vectors involving XMLHttpRequest and open of a file:/// URL, or discovering PostgreSQL passwords via vectors involving Window.localStorage and savedConnections. **CVE ID : CVE-2021-33570**	N/A	A-POS-POST-040621/185
Privoxy					
privoxy					
Missing Release of Memory after Effective Lifetime	25-May-21	5	A memory leak vulnerability was found in Privoxy before 3.0.29 in the show-status CGI handler when no action files are configured. **CVE ID : CVE-2021-20209**	https://www.privoxy.org/gitweb/?p=privoxy.git;a=commit;h=c62254a686, https://bugzilla.redhat.com/show_bug.cgi?id=1928726, https://www.privoxy.org/3.0.29/user-	A-PRI-PRIV-040621/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				manual/whatsnew.html	
Progress					
moveit_transfer					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-May-21	6.5	In Progress MOVEit Transfer before 2021.0 (13.0), a SQL injection vulnerability has been found in the MOVEit Transfer web app that could allow an authenticated attacker to gain unauthorized access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or destroy database elements. This is in MOVEit.DMZ.WebApp in SILHuman.vb. **CVE ID : CVE-2021-31827**	https://docs.ipswitch.com/MOVEit/Transfer2021/ReleaseNotes/en/index.htm, https://community.progress.com/s/article/MOVEit-Transfer-Vulnerability-April-2021, https://www.progress.com/moveit	A-PRO-MOVE-040621/187
prometheus					
prometheus					
URL Redirection to Untrusted Site ('Open Redirect')	19-May-21	5.8	Prometheus is an open-source monitoring system and time series database. In 2.23.0, Prometheus changed its default UI to the New ui. To ensure a seamless transition, the URL's prefixed by /new redirect to /. Due to a bug in the code, it is possible for an attacker to craft an URL that can redirect to any other URL,	https://github.com/prometheus/prometheus/security/advisories/GHSA-vx57-7f4q-fpc7	A-PRO-PROM-040621/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the /new endpoint. If a user visits a prometheus server with a specially crafted address, they can be redirected to an arbitrary URL. The issue was patched in the 2.26.1 and 2.27.1 releases. In 2.28.0, the /new endpoint will be removed completely. The workaround is to disable access to /new via a reverse proxy in front of Prometheus. **CVE ID : CVE-2021-29622**		
psyonix					
rocket_league					
Out-of-bounds Write	18-May-21	9.3	Epic Games / Psyonix Rocket League <=1.95 is affected by Buffer Overflow. Stack-based buffer overflow occurs when Rocket League handles UPK object files that can result in code execution and denial of service scenario. **CVE ID : CVE-2021-32238**	https://exchange.xforce.ibmcloud.com/vulnerabilities/201129	A-PSY-ROCK-040621/189
Putty					
putty					
N/A	21-May-21	5	PuTTY before 0.75 on Windows allows remote servers to cause a denial of service (Windows GUI hang) by telling the PuTTY window to change its title repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls. NOTE: the same attack methodology may affect some OS-level GUIs on Linux or other platforms for similar	N/A	A-PUT-PUTT-040621/190

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
			reasons. **CVE ID : CVE-2021-33500**		
Python					
python					
Exposure of Sensitive Information to an Unauthorized Actor	20-May-21	2.7	There's a flaw in Python 3's pydoc. A local or adjacent attacker who discovers or is able to convince another local or adjacent user to start a pydoc server could access the server and use it to disclose sensitive information belonging to the other user that they would not normally be able to access. The highest risk of this flaw is to data confidentiality. This flaw affects Python versions before 3.8.9, Python versions before 3.9.3 and Python versions before 3.10.0a7. **CVE ID : CVE-2021-3426**	https://bugzilla.redhat.com/show_bug.cgi?id=1935913	A-PYT-PYTH-040621/191
re-logic					
terraria					
Deserialization of Untrusted Data	24-May-21	7.5	Re-Logic Terraria before 1.4.2.3 performs Insecure Deserialization. **CVE ID : CVE-2021-32075**	N/A	A-RE--TERR-040621/192
Redhat					
build_of_quarkus					
Improper Neutralization of Input During Web Page Generation ('Cross-site	20-May-21	3.5	A flaw was found in Wildfly in versions before 23.0.2.Final while creating a new role in domain mode via the admin console, it is possible to add a payload in the name field, leading to XSS. This affects	https://bugzilla.redhat.com/show_bug.cgi?id=1948001	A-RED-BUIL-040621/193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Confidentiality and Integrity. **CVE ID : CVE-2021-3536**		
ceph					
Improper Input Validation	17-May-21	4.3	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway) in versions before 14.2.21. The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. In addition, the prior bug fix for CVE-2020-10753 did not account for the use of \r as a header separator, thus a new flaw has been created. **CVE ID : CVE-2021-3524**	https://bugzilla.redhat.com/show_bug.cgi?id=1951674	A-RED-CEPH-040621/194
Improper Input Validation	18-May-21	5	A flaw was found in the Red Hat Ceph Storage RGW in versions before 14.2.21. When processing a GET Request for a swift URL that ends with two slashes it can cause the rgw to crash, resulting in a denial of service. The greatest threat to the system is of availability. **CVE ID : CVE-2021-3531**	https://bugzilla.redhat.com/show_bug.cgi?id=1955326, http://www.openwall.com/lists/oss-security/2021/05/14/5, http://www.openwall.com/lists/oss-security/2021/05/17/7	A-RED-CEPH-040621/195
ceph_storage					
Improper	17-May-21	4.3	A flaw was found in the Red	https://bugz	A-RED-CEPH-

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
Input Validation			Hat Ceph Storage RadosGW (Ceph Object Gateway) in versions before 14.2.21. The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. In addition, the prior bug fix for CVE-2020-10753 did not account for the use of \r as a header separator, thus a new flaw has been created. **CVE ID : CVE-2021-3524**	illa.redhat.com/show_bug.cgi?id=1951674	040621/196
Improper Input Validation	18-May-21	5	A flaw was found in the Red Hat Ceph Storage RGW in versions before 14.2.21. When processing a GET Request for a swift URL that ends with two slashes it can cause the rgw to crash, resulting in a denial of service. The greatest threat to the system is of availability. **CVE ID : CVE-2021-3531**	https://bugzilla.redhat.com/show_bug.cgi?id=1955326, http://www.openwall.com/lists/oss-security/2021/05/14/5, http://www.openwall.com/lists/oss-security/2021/05/17/7	A-RED-CEPH-040621/197
data_grid					
Improper Neutralization of Input During Web Page Generation	20-May-21	3.5	A flaw was found in Wildfly in versions before 23.0.2.Final while creating a new role in domain mode via the admin console, it is possible to add a payload in the name field,	https://bugzilla.redhat.com/show_bug.cgi?id=1948001	A-RED-DATA-040621/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			leading to XSS. This affects Confidentiality and Integrity. **CVE ID : CVE-2021-3536**		
descision_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	3.5	A flaw was found in Wildfly in versions before 23.0.2.Final while creating a new role in domain mode via the admin console, it is possible to add a payload in the name field, leading to XSS. This affects Confidentiality and Integrity. **CVE ID : CVE-2021-3536**	https://bugzilla.redhat.com/show_bug.cgi?id=1948001	A-RED-DESC-040621/199
integration_camel_k					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	3.5	A flaw was found in Wildfly in versions before 23.0.2.Final while creating a new role in domain mode via the admin console, it is possible to add a payload in the name field, leading to XSS. This affects Confidentiality and Integrity. **CVE ID : CVE-2021-3536**	https://bugzilla.redhat.com/show_bug.cgi?id=1948001	A-RED-INTE-040621/200
integration_camel_quarkus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	3.5	A flaw was found in Wildfly in versions before 23.0.2.Final while creating a new role in domain mode via the admin console, it is possible to add a payload in the name field, leading to XSS. This affects Confidentiality and Integrity. **CVE ID : CVE-2021-3536**	https://bugzilla.redhat.com/show_bug.cgi?id=1948001	A-RED-INTE-040621/201
integration_service_registry					
Improper Neutralization of Input	20-May-21	3.5	A flaw was found in Wildfly in versions before 23.0.2.Final while creating a new role in	https://bugzilla.redhat.com/show_bug	A-RED-INTE-040621/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			domain mode via the admin console, it is possible to add a payload in the name field, leading to XSS. This affects Confidentiality and Integrity. **CVE ID : CVE-2021-3536**	.cgi?id=1948001	
jboss_a-mq					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	3.5	A flaw was found in Wildfly in versions before 23.0.2.Final while creating a new role in domain mode via the admin console, it is possible to add a payload in the name field, leading to XSS. This affects Confidentiality and Integrity. **CVE ID : CVE-2021-3536**	https://bugzilla.redhat.com/show_bug.cgi?id=1948001	A-RED-JBOS-040621/203
jboss_core_services					
Out-of-bounds Write	19-May-21	7.5	There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is able to supply a crafted file to be processed by an application linked with the affected functionality of libxml2 could trigger an out-of-bounds read. The most likely impact of this flaw is to application availability, with some potential impact to confidentiality and integrity if an attacker is able to use memory information to further exploit the application. **CVE ID : CVE-2021-3517**	https://bugzilla.redhat.com/show_bug.cgi?id=1954232	A-RED-JBOS-040621/204
Use After Free	18-May-21	6.8	There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed	https://bugzilla.redhat.com/show_bug.cgi?id=1954	A-RED-JBOS-040621/205

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
			by an application linked with libxml2 could trigger a use-after-free. The greatest impact from this flaw is to confidentiality, integrity, and availability. **CVE ID : CVE-2021-3518**	242	
jboss_enterprise_application_platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	3.5	A flaw was found in Wildfly in versions before 23.0.2.Final while creating a new role in domain mode via the admin console, it is possible to add a payload in the name field, leading to XSS. This affects Confidentiality and Integrity. **CVE ID : CVE-2021-3536**	https://bugzilla.redhat.com/show_bug.cgi?id=1948001	A-RED-JBOS-040621/206
software_collections					
Exposure of Sensitive Information to an Unauthorized Actor	20-May-21	2.7	There's a flaw in Python 3's pydoc. A local or adjacent attacker who discovers or is able to convince another local or adjacent user to start a pydoc server could access the server and use it to disclose sensitive information belonging to the other user that they would not normally be able to access. The highest risk of this flaw is to data confidentiality. This flaw affects Python versions before 3.8.9, Python versions before 3.9.3 and Python versions before 3.10.0a7. **CVE ID : CVE-2021-3426**	https://bugzilla.redhat.com/show_bug.cgi?id=1935913	A-RED-SOFT-040621/207
wildfly					
Improper	20-May-21	3.5	A flaw was found in Wildfly in	https://bugz	A-RED-WILD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			versions before 23.0.2.Final while creating a new role in domain mode via the admin console, it is possible to add a payload in the name field, leading to XSS. This affects Confidentiality and Integrity. **CVE ID : CVE-2021-3536**	illa.redhat.com/show_bug.cgi?id=1948001	040621/208
ronomon					
opened					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-May-21	10	The @ronomon/opened library before 1.5.2 is vulnerable to a command injection vulnerability which would allow a remote attacker to execute commands on the system if the library was used with untrusted input. **CVE ID : CVE-2021-29300**	https://github.com/ronomon/opened/commit/7effe011d4fea8fac7f78c00615e0a6e69af68ec	A-RON-OPEN-040621/209
RSA					
archer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-May-21	3.5	RSA Archer before 6.9 SP1 P1 (6.9.1.1) contains a stored XSS vulnerability. A remote authenticated malicious Archer user with access to modify link name fields could potentially exploit this vulnerability to execute code in a victim's browser. **CVE ID : CVE-2021-29252**	https://www.rsa.com/en-us/company/vulnerability-response-policy, https://community.rsa.com/t5/archer-product-advisories/rsa-2021-04-archer-an-rsa-business-update-for-multiple/ta-	A-RSA-ARCH-040621/210

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
				p/603223	
rxvt-unicode_project					
rxvt-unicode					
Improper Handling of Exceptional Conditions	20-May-21	6.5	rxvt-unicode 9.22, rxvt 2.7.10, mrxvt 0.5.4, and Eterm 0.9.7 allow (potentially remote) code execution because of improper handling of certain escape sequences (ESC G Q). A response is terminated by a newline. **CVE ID : CVE-2021-33477**	http://cvs.schmorp.de/rxvt-unicode/src/command.C?r1=1.582&r2=1.583	A-RXV-RXVT-040621/211
rxvt_project					
rxvt					
Improper Handling of Exceptional Conditions	20-May-21	6.5	rxvt-unicode 9.22, rxvt 2.7.10, mrxvt 0.5.4, and Eterm 0.9.7 allow (potentially remote) code execution because of improper handling of certain escape sequences (ESC G Q). A response is terminated by a newline. **CVE ID : CVE-2021-33477**	http://cvs.schmorp.de/rxvt-unicode/src/command.C?r1=1.582&r2=1.583	A-RXV-RXVT-040621/212
Shopizer					
shopizer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	3.5	A stored cross-site scripting (XSS) vulnerability in Shopizer before 2.17.0 allows remote attackers to inject arbitrary web script or HTML via customer_name in various forms of store administration. It is saved in the database. The code is executed for any user of store administration when information is fetched from the backend, e.g., in	https://github.com/shopizer-ecommerce/shopizer/compare/2.16.0...2.17.0, https://github.com/shopizer-ecommerce/shopizer/commit/197f8c	A-SHO-SHOP-040621/213

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
			admin/customers/list.html. **CVE ID : CVE-2021-33561**	78c8f673b957e41ca2c823afc654c19271	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	3.5	A reflected cross-site scripting (XSS) vulnerability in Shopizer before 2.17.0 allows remote attackers to inject arbitrary web script or HTML via the ref parameter to a page about an arbitrary product, e.g., a product/insert-product-name-here.html/ref=URL. **CVE ID : CVE-2021-33562**	https://github.com/shopizer-ecommerce/shopizer/compare/2.16.0...2.17.0, https://github.com/shopizer-ecommerce/shopizer/commit/197f8c78c8f673b957e41ca2c823afc654c19271	A-SHO-SHOP-040621/214
slapi-nis_project					
slapi-nis					
NULL Pointer Dereference	20-May-21	5	A flaw was found in slapi-nis in versions before 0.56.7. A NULL pointer dereference during the parsing of the Binding DN could allow an unauthenticated attacker to crash the 389-ds-base directory server. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2021-3480**	https://bugzilla.redhat.com/show_bug.cgi?id=1944640	A-SLA-SLAP-040621/215
Solarwinds					
network_performance_monitor					
Deserialization of Untrusted	21-May-21	10	This vulnerability allows remote attackers to execute arbitrary code on affected	https://documentation.solarwinds.co	A-SOL-NETW-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Data			installations of SolarWinds Network Performance Monitor 2020.2.1. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SolarWinds.Serialization library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-12213. **CVE ID : CVE-2021-31474**	m/en/success_center/sam/content/release_notes/sam_2020-2-5_release_notes.htm	040621/216
Sophos					
home					
Improper Control of Generation of Code ('Code Injection')	17-May-21	7.2	In multiple versions of Sophos Endpoint products for MacOS, a local attacker could execute arbitrary code with administrator privileges. **CVE ID : CVE-2021-25264**	https://community.sophos.com/b/security-blog/posts/resolved-lpe-in-endpoint-for-macos-cve-2021-25264, https://community.sophos.com/b/security-blog	A-SOP-HOME-040621/217
intercept_x					
Improper Control of Generation of Code ('Code	17-May-21	7.2	In multiple versions of Sophos Endpoint products for MacOS, a local attacker could execute arbitrary code with administrator privileges.	https://community.sophos.com/b/security-blog/posts/r	A-SOP-INTE-040621/218

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
Injection')			**CVE ID : CVE-2021-25264**	esolved-lpe-in-endpoint-for-macos-cve-2021-25264, https://community.sophos.com/b/security-blog	
Synology					
diskstation_manager					
Heap-based Buffer Overflow	21-May-21	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Synology DiskStation Manager. Authentication is not required to exploit this vulnerablity. The specific flaw exists within the processing of DSI structures in Netatalk. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12326. **CVE ID : CVE-2021-31439**	https://www.synology.com/zh-hk/security/advisory/Synology_SA_20_26	A-SYN-DISK-040621/219
targetfirst					
watcheezy					
Improper Neutralization of Input During Web Page Generation	24-May-21	4.3	The Target First WordPress Plugin v2.0, also previously known as Watcheezy, suffers from a critical unauthenticated stored XSS vulnerability. An attacker	https://www.targetfirst.com/, https://wpscan.com/vulnerability/4d5	A-TAR-WATC-040621/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could change the licence key value through a POST on any URL with the 'weeWzKey' parameter that will be save as the 'weeID option and is not sanitized. **CVE ID : CVE-2021-24305**	5d1f5-a7b8-4029-942d-7a13e2498f64	
Telegram					
telegram					
Out-of-bounds Write	18-May-21	4.3	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Stack Based Overflow in the blit function of their custom fork of the rlottie library. A remote attacker might be able to access Telegram's stack memory out-of-bounds on a victim device via a malicious animated sticker. **CVE ID : CVE-2021-31315**	N/A	A-TEL-TELE-040621/221
Access of Resource Using Incompatible Type ('Type Confusion')	18-May-21	4.3	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Type Confusion in the VDasher constructor of their custom fork of the rlottie library. A remote attacker might be able to access Telegram's heap memory out-of-bounds on a victim device via a malicious animated sticker. **CVE ID : CVE-2021-31317**	N/A	A-TEL-TELE-040621/222
Access of Resource Using Incompatible	18-May-21	4.3	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Type Confusion	N/A	A-TEL-TELE-040621/223

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
Type ('Type Confusion')			in the LOTCompLayerItem::LOTCompLayerItem function of their custom fork of the rlottie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker. **CVE ID : CVE-2021-31318**		
Integer Overflow or Wraparound	18-May-21	4.3	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by an Integer Overflow in the LOTGradient::populate function of their custom fork of the rlottie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker. **CVE ID : CVE-2021-31319**	N/A	A-TEL-TELE-040621/224
Out-of-bounds Write	18-May-21	5.8	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Heap Buffer Overflow in the VGradientCache::generateGradientColorTable function of their custom fork of the rlottie library. A remote attacker might be able to overwrite heap memory out-of-bounds on a victim device via a malicious animated sticker. **CVE ID : CVE-2021-31320**	N/A	A-TEL-TELE-040621/225
Out-of-bounds	18-May-21	5.8	Telegram Android <7.1.0 (2090), Telegram iOS <7.1,	N/A	A-TEL-TELE-040621/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			and Telegram macOS <7.1 are affected by a Stack Based Overflow in the gray_split_cubic function of their custom fork of the rlottie library. A remote attacker might be able to overwrite Telegram's stack memory out-of-bounds on a victim device via a malicious animated sticker. **CVE ID : CVE-2021-31321**		
Out-of-bounds Write	18-May-21	4.3	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Heap Buffer Overflow in the LOTGradient::populate function of their custom fork of the rlottie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker. **CVE ID : CVE-2021-31322**	N/A	A-TEL-TELE-040621/227
Out-of-bounds Write	18-May-21	4.3	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Heap Buffer Overflow in the LottieParserImpl::parseDashProperty function of their custom fork of the rlottie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker. **CVE ID : CVE-2021-31323**	N/A	A-TEL-TELE-040621/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
telop01_project					
telop01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	4.3	Reflected cross-site scripting vulnerability in the admin page of [Telop01] free edition ver1.0.1 and earlier allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20724**	N/A	A-TEL-TELO-040621/229
trailing-slash_project					
trailing-slash					
URL Redirection to Untrusted Site ('Open Redirect')	24-May-21	5.8	The package trailing-slash before 2.0.1 are vulnerable to Open Redirect via the use of trailing double slashes in the URL when accessing the vulnerable endpoint (such as https://example.com//attacker.example/). The vulnerable code is in index.js::createTrailing(), as the web server uses relative URLs instead of absolute URLs. **CVE ID : CVE-2021-23387**	https://snyk.io/vuln/SNYK-JS-TRAILINGSLASH-1085707, https://github.com/fardog/trailing-slash/commit/f8e66f1429308247e5a119d430203077d8f05048	A-TRA-TRAI-040621/230
Trendmicro					
home_network_security					
Improper Privilege Management	26-May-21	4.6	A privilege escalation vulnerability exists in the tdts.ko chrdev_ioctl_handle functionality of Trend Micro, Inc. Home Network Security 6.1.567. A specially crafted ioctl can lead to increased privileges. An attacker can issue an ioctl to trigger this	N/A	A-TRE-HOME-040621/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. **CVE ID : CVE-2021-32457**		
unified-automation					
.net_based_opc_ua_client\\/server_sdk					
Exposure of Sensitive Information to an Unauthorized Actor	20-May-21	5	Products with Unified Automation .NET based OPC UA Client/Server SDK Bundle: Versions V3.0.7 and prior (.NET 4.5, 4.0, and 3.5 Framework versions only) are vulnerable to an uncontrolled recursion, which may allow an attacker to trigger a stack overflow. **CVE ID : CVE-2021-27434**	N/A	A-UNI-.NET-040621/232
vmd_project					
vmd					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	4.3	vmd through 1.34.0 allows 'div class="markdown-body"' XSS, as demonstrated by Electron remote code execution via require('child_process').execSync('calc.exe') on Windows and a similar attack on macOS. **CVE ID : CVE-2021-33041**	N/A	A-VMD-VMD-040621/233
Vmware					
rabbitmq					
Improper Control of Generation of Code ('Code Injection')	18-May-21	4.6	RabbitMQ installers on Windows prior to version 3.8.16 do not harden plugin directory permissions, potentially allowing attackers with sufficient local filesystem permissions to add arbitrary plugins. **CVE ID : CVE-2021-22117**	https://tanzu.vmware.com/security/cve-2021-22117	A-VMW-RABB-040621/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
webfairy					
mediat					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-21	4.3	An issue was discovered in Mediat 1.4.1. There is a Reflected XSS vulnerability which allows remote attackers to inject arbitrary web script or HTML without authentication via the 'return' parameter in login.php. **CVE ID : CVE-2021-30083**	N/A	A-WEB-MEDI-040621/235
Websvn					
websvn					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-May-21	10	WebSVN before 2.6.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the search parameter. **CVE ID : CVE-2021-32305**	https://github.com/websvnphp/websvn/pull/142	A-WEB-WEBS-040621/236
wedevs					
happy_addons_for_elementor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	3.5	The Happy Addons for Elementor WordPress plugin before 2.24.0, Happy Addons Pro for Elementor WordPress plugin before 1.17.0 have a number of widgets that are vulnerable to stored Cross-Site Scripting(XSS) by lower-privileged users such as contributors, all via a similar method: The “Card” widget accepts a “title_tag” parameter. Although the element control lists a fixed	https://wpscan.com/vulnerability/0f20e098-8106-451f-9448-d35a79f03077	A-WED-HAPP-040621/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			set of possible html tags, it is possible to send a 'save_builder' request with the "heading_tag" set to "script", and the actual "title" parameter set to JavaScript to be executed within the script tags added by the "heading_tag" parameter. **CVE ID : CVE-2021-24292**		
Woocommerce					
woocommerce					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-21	3.5	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privilege users such as admin to use XSS payloads even when the unfiltered_html is disabled **CVE ID : CVE-2021-24323**	https://wpscan.com/vulnerability/6d262555-7ae4-4e36-add6-4baa34dc3010	A-WOO-WOOC-040621/238
Xmlsoft					
libxml2					
Out-of-bounds Write	19-May-21	7.5	There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is able to supply a crafted file to be processed by an application linked with the affected functionality of libxml2 could trigger an out-of-bounds read. The most likely impact of this flaw is to application availability, with some potential impact to confidentiality and integrity if an attacker is able to use	https://bugzilla.redhat.com/show_bug.cgi?id=1954232	A-XML-LIBX-040621/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory information to further exploit the application. **CVE ID : CVE-2021-3517**		
Use After Free	18-May-21	6.8	There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by an application linked with libxml2 could trigger a use-after-free. The greatest impact from this flaw is to confidentiality, integrity, and availability. **CVE ID : CVE-2021-3518**	https://bugzilla.redhat.com/show_bug.cgi?id=1954242	A-XML-LIBX-040621/240
zettlr					
zettlr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-May-21	4.3	Cross-site scripting vulnerability in Zettlr from 0.20.0 to 1.8.8 allows an attacker to execute an arbitrary script by loading a file or code snippet containing an invalid iframe into Zettlr. **CVE ID : CVE-2021-20727**	N/A	A-ZET-ZETT-040621/241
zmartzone					
mod_auth_openidc					
Uncontrolled Resource Consumption	20-May-21	5	mod_auth_openidc 2.4.0 to 2.4.7 allows a remote attacker to cause a denial-of-service (DoS) condition via unspecified vectors. **CVE ID : CVE-2021-20718**	https://www.zmartzone.eu/	A-ZMA-MOD_-040621/242
Zohocorp					
manageengine_adselfservice_plus					
Improper Neutralization of Input	20-May-21	4.3	Zoho ManageEngine ADSelfService Plus before 6104 allows stored XSS on the	https://pitstop.manageengine.com/po	A-ZOH-MANA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			/webclient/index.html#/directory-search user search page via the e-mail address field. **CVE ID : CVE-2021-27956**	rtal/en/community/topic/adselfservice-plus-6104-released-with-an-important-security-fixes, https://www.manageengine.com	040621/243
Zope					
Zope					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-May-21	6.5	Zope is an open-source web application server. In Zope versions prior to 4.6 and 5.2, users can access untrusted modules indirectly through Python modules that are available for direct use. By default, only users with the Manager role can add or edit Zope Page Templates through the web, but sites that allow untrusted users to add/edit Zope Page Templates through the web are at risk from this vulnerability. The problem has been fixed in Zope 5.2 and 4.6. As a workaround, a site administrator can restrict adding/editing Zope Page Templates through the web using the standard Zope user/role permission mechanisms. Untrusted users should not be assigned the Zope Manager role and adding/editing Zope Page	https://github.com/zopefoundation/Zope/commit/1f8456bf1f908ea46012537d52bd7e752a532c91, https://github.com/zopefoundation/Zope/security/advisories/GHSA-5pr9-v234-jw36	A-ZOP-ZOPE-040621/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Templates through the web should be restricted to trusted users only. **CVE ID : CVE-2021-32633**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-May-21	4.3	Zope Products.CMFCore before 2.5.1 and Products.PluggableAuthService before 2.6.2, as used in Plone through 5.2.4 and other products, allow Reflected XSS. **CVE ID : CVE-2021-33507**	https://plone.org/security/hotfix/20210518/reflected-xss-in-various-spots	A-ZOP-ZOPE-040621/245
ZTE					
zxcdn					
Exposure of Sensitive Information to an Unauthorized Actor	19-May-21	4	The management system of ZXCDN is impacted by the information leak vulnerability. Attackers can make further analysis according to the information returned by the program, and then obtain some sensitive information. This affects ZXCDN V7.01 all versions up to IAMV7.01.01.02. **CVE ID : CVE-2021-21733**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1015304	A-ZTE-ZXCD-040621/246
Hardware					
Cisco					
wap125					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/247

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
			affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/249
Improper Neutralization of Special Elements used in a Command	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-WAP1-040621/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**	sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1551**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/252
Improper Neutralization of Special	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco	https://tools.cisco.com/security/center	H-CIS-WAP1-040621/253

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
Elements used in a Command ('Command Injection')			Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**	/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1555**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/255

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
wap131					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/256
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/259
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-	H-CIS-WAP1-040621/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1551**	Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/262
Improper Neutralization of Special Elements used in a	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access	https://tools.cisco.com/security/center/content/CiscoSecurityAd	H-CIS-WAP1-040621/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**	visory/cisco-sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1555**		
wap150					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/266
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the device. **CVE ID : CVE-2021-1550**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1551**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/269
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/270

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
			vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP1-040621/272
Improper Neutralization of Special Elements used in a Command ('Command	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-	H-CIS-WAP1-040621/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1555**	inject-Mp9FSdG	
wap351					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/275
Improper Neutralizatio	22-May-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/se	H-CIS-WAP3-040621/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1551		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/279
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1555**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/282
wap361					
Improper Neutralization of Special Elements used in a Command ('Command	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-	H-CIS-WAP3-040621/283

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
Injection')			attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**	inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/285
Improper Neutralization of Special Elements	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and	https://tools.cisco.com/security/center/content/Cis	H-CIS-WAP3-040621/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**	coSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1551**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/288
Improper	22-May-21	9	Multiple vulnerabilities in the	https://tools.	H-CIS-WAP3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	040621/289
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP3-040621/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the device. **CVE ID : CVE-2021-1555**		
wap581					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP5-040621/292
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-	H-CIS-WAP5-040621/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**	Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP5-040621/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP5-040621/295
Improper Neutralization of Special Elements used in a Command	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-WAP5-040621/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1551**	sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP5-040621/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP5-040621/298
Improper Neutralization of Special	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco	https://tools.cisco.com/security/center	H-CIS-WAP5-040621/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**	/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	H-CIS-WAP5-040621/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1555**		
Dell					
xtremio_x1					
Cross-Site Request Forgery (CSRF)	21-May-21	6.8	Dell EMC XtremIO Versions prior to 6.3.3-8, contain a Cross-Site Request Forgery Vulnerability in XMS. A non-privileged attacker could potentially exploit this vulnerability, leading to a privileged victim application user being tricked into sending state-changing requests to the vulnerable application, causing unintended server operations. **CVE ID : CVE-2021-21549**	https://www.dell.com/support/kbdoc/000186363	H-DEL-XTRE-040621/301
xtremio_x2					
Cross-Site Request Forgery (CSRF)	21-May-21	6.8	Dell EMC XtremIO Versions prior to 6.3.3-8, contain a Cross-Site Request Forgery Vulnerability in XMS. A non-privileged attacker could potentially exploit this vulnerability, leading to a privileged victim application user being tricked into sending state-changing	https://www.dell.com/support/kbdoc/000186363	H-DEL-XTRE-040621/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests to the vulnerable application, causing unintended server operations. **CVE ID : CVE-2021-21549**		
Dlink					
dir-842e					
Observable Discrepancy	17-May-21	4.3	An authentication brute-force protection mechanism bypass in telnetd in D-Link Router model DIR-842 firmware version 3.0.2 allows a remote attacker to circumvent the anti-brute-force cool-down delay period via a timing-based side-channel attack **CVE ID : CVE-2021-27342**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10225	H-DLI-DIR--040621/303
draeger					
x-dock_5300					
Use of Hard-coded Credentials	20-May-21	6.5	Draeger X-Dock Firmware before 03.00.13 has Hard-Coded Credentials, leading to remote code execution by an authenticated attacker. **CVE ID : CVE-2021-28111**	https://static.draeger.com/security, https://static.draeger.com/security/download/PSA-21-120-1-X-Dock-Product-Security-Advisory.pdf	H-DRA-X-DO-040621/304
N/A	20-May-21	6.5	Draeger X-Dock Firmware before 03.00.13 has Active Debug Code on a debug port, leading to remote code execution by an authenticated attacker. **CVE ID : CVE-2021-28112**	https://static.draeger.com/security, https://static.draeger.com/security/download/PSA-21-120-	H-DRA-X-DO-040621/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1-X-Dock-Product-Security-Advisory.pdf	
x-dock_6300					
Use of Hard-coded Credentials	20-May-21	6.5	Draeger X-Dock Firmware before 03.00.13 has Hard-Coded Credentials, leading to remote code execution by an authenticated attacker. **CVE ID : CVE-2021-28111**	https://static.draeger.com/security, https://static.draeger.com/security/download/PSA-21-120-1-X-Dock-Product-Security-Advisory.pdf	H-DRA-X-DO-040621/306
N/A	20-May-21	6.5	Draeger X-Dock Firmware before 03.00.13 has Active Debug Code on a debug port, leading to remote code execution by an authenticated attacker. **CVE ID : CVE-2021-28112**	https://static.draeger.com/security, https://static.draeger.com/security/download/PSA-21-120-1-X-Dock-Product-Security-Advisory.pdf	H-DRA-X-DO-040621/307
x-dock_6600					
Use of Hard-coded Credentials	20-May-21	6.5	Draeger X-Dock Firmware before 03.00.13 has Hard-Coded Credentials, leading to remote code execution by an authenticated attacker. **CVE ID : CVE-2021-28111**	https://static.draeger.com/security, https://static.draeger.com/security/download/PSA-21-120-1-X-Dock-Product-	H-DRA-X-DO-040621/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				Security-Advisory.pdf	
N/A	20-May-21	6.5	Draeger X-Dock Firmware before 03.00.13 has Active Debug Code on a debug port, leading to remote code execution by an authenticated attacker. **CVE ID : CVE-2021-28112**	https://static.draeger.com/security, https://static.draeger.com/security/download/PSA-21-120-1-X-Dock-Product-Security-Advisory.pdf	H-DRA-X-DO-040621/309
Emerson					
x-stream_enhanced_xefd					
Inadequate Encryption Strength	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for storage of sensitive data, which may allow an attacker to more easily obtain credentials used for access. **CVE ID : CVE-2021-27457**	N/A	H-EME-X-ST-040621/310
Unrestricted Upload of File with Dangerous Type	20-May-21	7.5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an attacker could utilize to execute arbitrary code. **CVE ID : CVE-2021-27459**	N/A	H-EME-X-ST-040621/311
Improper Limitation of	20-May-21	5	A vulnerability has been found in multiple revisions of	N/A	H-EME-X-ST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver applications allow access to stored data that can be obtained by using specially crafted URLs. **CVE ID : CVE-2021-27461**		040621/312
Use of Persistent Cookies Containing Sensitive Information	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the session cookie attribute is not properly invalidated, allowing an attacker to intercept the cookies and gain access to sensitive information. **CVE ID : CVE-2021-27463**	N/A	H-EME-X-ST-040621/313
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	4.3	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not validate webpage input, which could allow an attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data. **CVE ID : CVE-2021-27465**	N/A	H-EME-X-ST-040621/314
Improper Restriction of Rendered UI Layers or Frames	20-May-21	5.8	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product's web interface allows an attacker to	N/A	H-EME-X-ST-040621/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			route click or keystroke to another page provided by the attacker to gain unauthorized access to sensitive information. **CVE ID : CVE-2021-27467**		
x-stream_enhanced_xegk					
Inadequate Encryption Strength	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for storage of sensitive data, which may allow an attacker to more easily obtain credentials used for access. **CVE ID : CVE-2021-27457**	N/A	H-EME-X-ST-040621/316
Unrestricted Upload of File with Dangerous Type	20-May-21	7.5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an attacker could utilize to execute arbitrary code. **CVE ID : CVE-2021-27459**	N/A	H-EME-X-ST-040621/317
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver applications allow access to stored data that can be obtained by using specially crafted URLs. **CVE ID : CVE-2021-27461**	N/A	H-EME-X-ST-040621/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Persistent Cookies Containing Sensitive Information	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the session cookie attribute is not properly invalidated, allowing an attacker to intercept the cookies and gain access to sensitive information. **CVE ID : CVE-2021-27463**	N/A	H-EME-X-ST-040621/319
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	4.3	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not validate webpage input, which could allow an attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data. **CVE ID : CVE-2021-27465**	N/A	H-EME-X-ST-040621/320
Improper Restriction of Rendered UI Layers or Frames	20-May-21	5.8	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product's web interface allows an attacker to route click or keystroke to another page provided by the attacker to gain unauthorized access to sensitive information. **CVE ID : CVE-2021-27467**	N/A	H-EME-X-ST-040621/321
x-stream_enhanced_xegp					
Inadequate	20-May-21	5	A vulnerability has been found	N/A	H-EME-X-ST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Encryption Strength			in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for storage of sensitive data, which may allow an attacker to more easily obtain credentials used for access. **CVE ID : CVE-2021-27457**		040621/322
Unrestricted Upload of File with Dangerous Type	20-May-21	7.5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an attacker could utilize to execute arbitrary code. **CVE ID : CVE-2021-27459**	N/A	H-EME-X-ST-040621/323
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver applications allow access to stored data that can be obtained by using specially crafted URLs. **CVE ID : CVE-2021-27461**	N/A	H-EME-X-ST-040621/324
Use of Persistent Cookies Containing Sensitive Information	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the session cookie attribute is not properly invalidated, allowing an attacker to intercept the	N/A	H-EME-X-ST-040621/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cookies and gain access to sensitive information. **CVE ID : CVE-2021-27463**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	4.3	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not validate webpage input, which could allow an attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data. **CVE ID : CVE-2021-27465**	N/A	H-EME-X-ST-040621/326
Improper Restriction of Rendered UI Layers or Frames	20-May-21	5.8	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product's web interface allows an attacker to route click or keystroke to another page provided by the attacker to gain unauthorized access to sensitive information. **CVE ID : CVE-2021-27467**	N/A	H-EME-X-ST-040621/327
x-stream_enhanced_xexf					
Inadequate Encryption Strength	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for storage of sensitive data, which may allow an attacker to more easily obtain credentials used for access.	N/A	H-EME-X-ST-040621/328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27457		
Unrestricted Upload of File with Dangerous Type	20-May-21	7.5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an attacker could utilize to execute arbitrary code. **CVE ID : CVE-2021-27459**	N/A	H-EME-X-ST-040621/329
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver applications allow access to stored data that can be obtained by using specially crafted URLs. **CVE ID : CVE-2021-27461**	N/A	H-EME-X-ST-040621/330
Use of Persistent Cookies Containing Sensitive Information	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the session cookie attribute is not properly invalidated, allowing an attacker to intercept the cookies and gain access to sensitive information. **CVE ID : CVE-2021-27463**	N/A	H-EME-X-ST-040621/331
Improper Neutralization of Input During Web Page Generation	20-May-21	4.3	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not validate webpage input, which	N/A	H-EME-X-ST-040621/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could allow an attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data. **CVE ID : CVE-2021-27465**		
Improper Restriction of Rendered UI Layers or Frames	20-May-21	5.8	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product's web interface allows an attacker to route click or keystroke to another page provided by the attacker to gain unauthorized access to sensitive information. **CVE ID : CVE-2021-27467**	N/A	H-EME-X-ST-040621/333
IBM					
8335-gca					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-May-21	8.5	IBM Host firmware for LC-class Systems could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request that would allow them to delete arbitrary files on the system. IBM X-Force ID: 200558. **CVE ID : CVE-2021-29695**	https://www.ibm.com/support/pages/node/6454303, https://exchange.xforce.ibmcloud.com/vulnerabilities/200558	H-IBM-8335-040621/334
8335-gta					
Improper Limitation of a Pathname to a Restricted	25-May-21	8.5	IBM Host firmware for LC-class Systems could allow a remote attacker to traverse directories on the system. An attacker could send a	https://www.ibm.com/support/pages/node/6454303,	H-IBM-8335-040621/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			specially-crafted URL request that would allow them to delete arbitrary files on the system. IBM X-Force ID: 200558. **CVE ID : CVE-2021-29695**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200558	
8335-gtb					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-May-21	8.5	IBM Host firmware for LC-class Systems could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request that would allow them to delete arbitrary files on the system. IBM X-Force ID: 200558. **CVE ID : CVE-2021-29695**	https://www.ibm.com/support/pages/node/6454303, https://exchange.xforce.ibmcloud.com/vulnerabilities/200558	H-IBM-8335-040621/336
intelbras					
rf_301k					
Cross-Site Request Forgery (CSRF)	17-May-21	6.8	Intelbras Router RF 301K Firmware 1.1.2 is vulnerable to Cross Site Request Forgery (CSRF) due to lack of validation and insecure configurations in inputs and modules. **CVE ID : CVE-2021-32402**	N/A	H-INT-RF_3-040621/337
Cross-Site Request Forgery (CSRF)	17-May-21	6.8	Intelbras Router RF 301K Firmware 1.1.2 is vulnerable to Cross Site Request Forgery (CSRF) due to lack of security mechanisms for token protection and unsafe inputs and modules. **CVE ID : CVE-2021-32403**	N/A	H-INT-RF_3-040621/338
Netgear					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gc108p					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-GC10-040621/339
gc108pp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-	H-NET-GC10-040621/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	
gs108t					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-GS10-040621/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
gs110tp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-GS11-040621/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
gs110tpp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-GS11-040621/343
gs110tup					
Improper Neutralization of Special	21-May-21	10	Certain NETGEAR devices are affected by command injection by an	https://kb.netgear.com/000063641/S	H-NET-GS11-040621/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	ecurity-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	
gs710tup					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-	H-NET-GS71-040621/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	Smart-Switches-PSV-2021-0071	
gs716tp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-GS71-040621/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
gs716tpp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-GS71-040621/347

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
gs724tp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-GS72-040621/348
gs724tpp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-	H-NET-GS72-040621/349

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
Injection')			setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	
gs728tp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-GS72-040621/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
gs728tpp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-GS72-040621/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
gs752tp					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-GS75-040621/352
gs752tpp					
Improper Neutralization of Special	21-May-21	10	Certain NETGEAR devices are affected by command injection by an	https://kb.netgear.com/000063641/S	H-NET-GS75-040621/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	ecurity-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	
ms510txm					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-	H-NET-MS51-040621/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	Smart-Switches-PSV-2021-0071	
ms510txup					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	H-NET-MS51-040621/355

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
			before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
nippon-antenna					
rfntps					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-May-21	7.7	RFNTPS firmware versions System_01000004 and earlier, and Web_01000004 and earlier allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors. **CVE ID : CVE-2021-20719**	https://www.nippon-antenna.co.jp/ja/news/news/news8217702780390204428.html	H-NIP-RFNT-040621/356
sitel-sa					
cap\\/prx					
Exposure of Sensitive Information to an Unauthorized Actor	17-May-21	2.1	SITEL CAP/PRX firmware version 5.2.01 allows an attacker with access to the local network, to access via HTTP to the internal configuration database of the device without any authentication. An attacker could exploit this vulnerability in order to obtain information about the device´s configuration. **CVE ID : CVE-2021-32453**	https://www.incibe-cert.es/en/early-warning/ics-advisories/sitel-capprx-information-exposure	H-SIT-CAP\-040621/357
Uncontrolled Resource	17-May-21	6.1	SITEL CAP/PRX firmware version 5.2.01, allows an	https://www.incibe-	H-SIT-CAP\-040621/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			attacker with access to the device´s network to cause a denial of service condition on the device. An attacker could exploit this vulnerability by sending HTTP requests massively. **CVE ID : CVE-2021-32455**	cert.es/en/early-warning/ics-advisories/sitel-capprx-vulnerable-denial-service-attack	
remote_cap\\/prx					
Use of Hard-coded Credentials	17-May-21	5.8	SITEL CAP/PRX firmware version 5.2.01 makes use of a hardcoded password. An attacker with access to the device could modify these credentials, leaving the administrators of the device without access. **CVE ID : CVE-2021-32454**	https://www.incibe-cert.es/en/early-warning/ics-advisories/sitel-capprx-hardcoded-credentials	H-SIT-REMO-040621/359
Cleartext Transmission of Sensitive Information	17-May-21	3.3	SITEL CAP/PRX firmware version 5.2.01 allows an attacker with access to the local network of the device to obtain the authentication passwords by analysing the network traffic. **CVE ID : CVE-2021-32456**	https://www.incibe-cert.es/en/early-warning/ics-advisories/sitel-capprx-cleartext-transmission-sensitive-information	H-SIT-REMO-040621/360
Wago					
750-8202					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			runtime. **CVE ID : CVE-2021-21000**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/362
750-8203					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/363
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/364
750-8204					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime.	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21000		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/366
750-8206					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/367
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/368
750-8207					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/370
750-8208					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/371
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/372
750-8210					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/373
Improper Limitation of	24-May-21	4	On WAGO PFC200 devices in different firmware versions	https://cert.vde.com/en-	H-WAG-750--040621/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	us/advisories/vde-2021-014	
750-8211					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/375
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/376
750-8212					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/377
Improper Limitation of a Pathname to a	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with	https://cert.vde.com/en-us/advisories/vde-2021-	H-WAG-750--040621/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	014	
750-8213					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/379
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/380
750-8214					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/381
Improper Limitation of a Pathname to a Restricted Directory	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			higher privileges. **CVE ID : CVE-2021-21001**		
750-8216					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/383
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/384
750-8217					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/385
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges.	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21001		
750-823					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/387
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/388
750-829					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/389
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
750-831					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/391
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/392
750-832					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/393
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/394
750-852					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/395
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/396
750-862					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/397
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/398
750-880					
Allocation of Resources	24-May-21	5	On WAGO PFC200 devices in different firmware versions	https://cert.vde.com/en-	H-WAG-750--040621/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	us/advisories/vde-2021-014	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/400
750-881					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/401
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/402
750-882					
Allocation of Resources Without Limits or	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network	https://cert.vde.com/en-us/advisories/vde-2021-	H-WAG-750--040621/403

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
Throttling			access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	014	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/404
750-885					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/405
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/406
750-889					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the login service of the runtime. **CVE ID : CVE-2021-21000**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/408
750-890					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/409
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/410
750-891					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime.	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21000		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/412
750-893					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/413
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	H-WAG-750--040621/414
ZTE					
axon_11_5g					
Incorrect Default Permissions	19-May-21	5	A mobile phone of ZTE is impacted by improper access control vulnerability. Due to improper permission settings, third-party applications can read some files in the proc file system without authorization. Attackers could exploit this vulnerability to obtain	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1015064	H-ZTE-AXON-040621/415

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
			sensitive information. This affects Axon 11 5G ZTE/CN_P725A12/P725A12:10/QKQ1.200816.002/20201116.175317:user/release-keys. **CVE ID : CVE-2021-21732**		
Operating System					
Belden					
hirschmann_hios					
Insufficiently Protected Credentials	17-May-21	7.5	Hirschmann HiOS 07.1.01, 07.1.02, and 08.1.00 through 08.5.xx and HiSecOS 03.3.00 through 03.5.01 allow remote attackers to change the credentials of existing users. **CVE ID : CVE-2021-27734**	https://dam.belden.com/dmm3bwsv3/assetstream.aspx?assetid=12914&mediaformatid=50063&destinationid=10016	O-BEL-HIRS-040621/416
hisecos					
Insufficiently Protected Credentials	17-May-21	7.5	Hirschmann HiOS 07.1.01, 07.1.02, and 08.1.00 through 08.5.xx and HiSecOS 03.3.00 through 03.5.01 allow remote attackers to change the credentials of existing users. **CVE ID : CVE-2021-27734**	https://dam.belden.com/dmm3bwsv3/assetstream.aspx?assetid=12914&mediaformatid=50063&destinationid=10016	O-BEL-HISE-040621/417
Cisco					
wap125_firmware					
Improper Neutralization of Special Elements used in a Command	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-WAP1-040621/418

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
('Command Injection')			authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**	sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/420
Improper Neutralization of Special	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco	https://tools.cisco.com/security/center	O-CIS-WAP1-040621/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**	/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1551**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/423

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
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/424
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the device. **CVE ID : CVE-2021-1555**		
wap131_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/427
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-	O-CIS-WAP1-040621/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**	Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/430
Improper Neutralization of Special Elements used in a Command	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-WAP1-040621/431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1551**	sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/433
Improper Neutralization of Special	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco	https://tools.cisco.com/security/center	O-CIS-WAP1-040621/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**	/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1555**		
wap150_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1547		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/437
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1551**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/440
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-	O-CIS-WAP1-040621/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**	Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/442

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
			with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP1-040621/443
Improper Neutralization of Special Elements used in a	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access	https://tools.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-WAP1-040621/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1555**	visory/cisco-sa-sb-wap-inject-Mp9FSdG	
wap351_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/447
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/448

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
			could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/449

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
			the device. **CVE ID : CVE-2021-1551**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/450
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/451

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
			vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1555**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/453
wap361_firmware					
Improper Neutralization of Special Elements used in a Command	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-WAP3-040621/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**	sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/456
Improper Neutralization of Special	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco	https://tools.cisco.com/security/center	O-CIS-WAP3-040621/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**	/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/458

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
			web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1551**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/460
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP3-040621/462

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
			the device. **CVE ID : CVE-2021-1555**		
wap581_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1547**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP5-040621/463
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-	O-CIS-WAP5-040621/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1548**	Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP5-040621/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1549**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1550**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP5-040621/466
Improper Neutralization of Special Elements used in a Command	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-WAP5-040621/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1551**	sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP5-040621/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1552**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1553**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP5-040621/469
Improper Neutralization of Special	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco	https://tools.cisco.com/security/center	O-CIS-WAP5-040621/470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1554**	/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-21	9	Multiple vulnerabilities in the web-based management interface of certain Cisco Small Business 100, 300, and 500 Series Wireless Access Points could allow an authenticated, remote attacker to perform command injection attacks against an affected device. These vulnerabilities are due to improper validation of user-supplied input. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG	O-CIS-WAP5-040621/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit these vulnerabilities, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2021-1555**		
Debian					
debian_linux					
Exposure of Sensitive Information to an Unauthorized Actor	26-May-21	5	An issue was discovered in management/commands/hyperkitty_import.py in HyperKitty through 1.3.4. When importing a private mailing list's archives, these archives are publicly visible for the duration of the import. For example, sensitive information might be available on the web for an hour during a large migration from Mailman 2 to Mailman 3. **CVE ID : CVE-2021-33038**	https://gitlab.com/mailman/hyperkitty/-/issues/380, https://gitlab.com/mailman/hyperkitty/-/commit/9025324597d60b2dff740e49b70b15589d6804fa	O-DEB-DEBI-040621/472
Exposure of Sensitive Information to an Unauthorized Actor	20-May-21	2.7	There's a flaw in Python 3's pydoc. A local or adjacent attacker who discovers or is able to convince another local or adjacent user to start a pydoc server could access the server and use it to disclose sensitive information belonging to the other user that they would not normally be able to access. The highest	https://bugzilla.redhat.com/show_bug.cgi?id=1935913	O-DEB-DEBI-040621/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			risk of this flaw is to data confidentiality. This flaw affects Python versions before 3.8.9, Python versions before 3.9.3 and Python versions before 3.10.0a7. **CVE ID : CVE-2021-3426**		
Out-of-bounds Write	19-May-21	7.5	There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is able to supply a crafted file to be processed by an application linked with the affected functionality of libxml2 could trigger an out-of-bounds read. The most likely impact of this flaw is to application availability, with some potential impact to confidentiality and integrity if an attacker is able to use memory information to further exploit the application. **CVE ID : CVE-2021-3517**	https://bugzilla.redhat.com/show_bug.cgi?id=1954232	O-DEB-DEBI-040621/474
Use After Free	18-May-21	6.8	There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by an application linked with libxml2 could trigger a use-after-free. The greatest impact from this flaw is to confidentiality, integrity, and availability. **CVE ID : CVE-2021-3518**	https://bugzilla.redhat.com/show_bug.cgi?id=1954242	O-DEB-DEBI-040621/475
Dlink					
dir-842e_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	17-May-21	4.3	An authentication brute-force protection mechanism bypass in telnetd in D-Link Router model DIR-842 firmware version 3.0.2 allows a remote attacker to circumvent the anti-brute-force cool-down delay period via a timing-based side-channel attack **CVE ID : CVE-2021-27342**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10225	O-DLI-DIR--040621/476
draeger					
x-dock_firmware					
Use of Hard-coded Credentials	20-May-21	6.5	Draeger X-Dock Firmware before 03.00.13 has Hard-Coded Credentials, leading to remote code execution by an authenticated attacker. **CVE ID : CVE-2021-28111**	https://static.draeger.com/security, https://static.draeger.com/security/download/PSA-21-120-1-X-Dock-Product-Security-Advisory.pdf	O-DRA-X-DO-040621/477
N/A	20-May-21	6.5	Draeger X-Dock Firmware before 03.00.13 has Active Debug Code on a debug port, leading to remote code execution by an authenticated attacker. **CVE ID : CVE-2021-28112**	https://static.draeger.com/security, https://static.draeger.com/security/download/PSA-21-120-1-X-Dock-Product-Security-Advisory.pdf	O-DRA-X-DO-040621/478
Emerson					
x-stream_enhanced_xefd_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for storage of sensitive data, which may allow an attacker to more easily obtain credentials used for access. **CVE ID : CVE-2021-27457**	N/A	O-EME-X-ST-040621/479
Unrestricted Upload of File with Dangerous Type	20-May-21	7.5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an attacker could utilize to execute arbitrary code. **CVE ID : CVE-2021-27459**	N/A	O-EME-X-ST-040621/480
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver applications allow access to stored data that can be obtained by using specially crafted URLs. **CVE ID : CVE-2021-27461**	N/A	O-EME-X-ST-040621/481
Use of Persistent Cookies Containing Sensitive Information	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the session cookie attribute is not properly invalidated, allowing	N/A	O-EME-X-ST-040621/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker to intercept the cookies and gain access to sensitive information. **CVE ID : CVE-2021-27463**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	4.3	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not validate webpage input, which could allow an attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data. **CVE ID : CVE-2021-27465**	N/A	O-EME-X-ST-040621/483
Improper Restriction of Rendered UI Layers or Frames	20-May-21	5.8	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product’s web interface allows an attacker to route click or keystroke to another page provided by the attacker to gain unauthorized access to sensitive information. **CVE ID : CVE-2021-27467**	N/A	O-EME-X-ST-040621/484
x-stream_enhanced_xegk_firmware					
Inadequate Encryption Strength	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for storage of sensitive data, which may allow an attacker to more easily obtain	N/A	O-EME-X-ST-040621/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials used for access. **CVE ID : CVE-2021-27457**		
Unrestricted Upload of File with Dangerous Type	20-May-21	7.5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an attacker could utilize to execute arbitrary code. **CVE ID : CVE-2021-27459**	N/A	O-EME-X-ST-040621/486
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver applications allow access to stored data that can be obtained by using specially crafted URLs. **CVE ID : CVE-2021-27461**	N/A	O-EME-X-ST-040621/487
Use of Persistent Cookies Containing Sensitive Information	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the session cookie attribute is not properly invalidated, allowing an attacker to intercept the cookies and gain access to sensitive information. **CVE ID : CVE-2021-27463**	N/A	O-EME-X-ST-040621/488
Improper Neutralization of Input During Web Page	20-May-21	4.3	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not	N/A	O-EME-X-ST-040621/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			validate webpage input, which could allow an attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data. **CVE ID : CVE-2021-27465**		
Improper Restriction of Rendered UI Layers or Frames	20-May-21	5.8	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product's web interface allows an attacker to route click or keystroke to another page provided by the attacker to gain unauthorized access to sensitive information. **CVE ID : CVE-2021-27467**	N/A	O-EME-X-ST-040621/490
x-stream_enhanced_xegp_firmware					
Inadequate Encryption Strength	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for storage of sensitive data, which may allow an attacker to more easily obtain credentials used for access. **CVE ID : CVE-2021-27457**	N/A	O-EME-X-ST-040621/491
Unrestricted Upload of File with Dangerous Type	20-May-21	7.5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an	N/A	O-EME-X-ST-040621/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could utilize to execute arbitrary code. **CVE ID : CVE-2021-27459**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver applications allow access to stored data that can be obtained by using specially crafted URLs. **CVE ID : CVE-2021-27461**	N/A	O-EME-X-ST-040621/493
Use of Persistent Cookies Containing Sensitive Information	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the session cookie attribute is not properly invalidated, allowing an attacker to intercept the cookies and gain access to sensitive information. **CVE ID : CVE-2021-27463**	N/A	O-EME-X-ST-040621/494
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	4.3	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not validate webpage input, which could allow an attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data. **CVE ID : CVE-2021-27465**	N/A	O-EME-X-ST-040621/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Rendered UI Layers or Frames	20-May-21	5.8	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product's web interface allows an attacker to route click or keystroke to another page provided by the attacker to gain unauthorized access to sensitive information. **CVE ID : CVE-2021-27467**	N/A	O-EME-X-ST-040621/496
x-stream_enhanced_xexf_firmware					
Inadequate Encryption Strength	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected products utilize a weak encryption algorithm for storage of sensitive data, which may allow an attacker to more easily obtain credentials used for access. **CVE ID : CVE-2021-27457**	N/A	O-EME-X-ST-040621/497
Unrestricted Upload of File with Dangerous Type	20-May-21	7.5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The webserver of the affected products allows unvalidated files to be uploaded, which an attacker could utilize to execute arbitrary code. **CVE ID : CVE-2021-27459**	N/A	O-EME-X-ST-040621/498
Improper Limitation of a Pathname to a Restricted	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected webserver	N/A	O-EME-X-ST-040621/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			applications allow access to stored data that can be obtained by using specially crafted URLs. **CVE ID : CVE-2021-27461**		
Use of Persistent Cookies Containing Sensitive Information	20-May-21	5	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications utilize persistent cookies where the session cookie attribute is not properly invalidated, allowing an attacker to intercept the cookies and gain access to sensitive information. **CVE ID : CVE-2021-27463**	N/A	O-EME-X-ST-040621/500
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-21	4.3	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected applications do not validate webpage input, which could allow an attacker to inject arbitrary HTML code into a webpage. This would allow an attacker to modify the page and display incorrect or undesirable data. **CVE ID : CVE-2021-27465**	N/A	O-EME-X-ST-040621/501
Improper Restriction of Rendered UI Layers or Frames	20-May-21	5.8	A vulnerability has been found in multiple revisions of Emerson Rosemount X-STREAM Gas Analyzer. The affected product's web interface allows an attacker to route click or keystroke to another page provided by the attacker to gain unauthorized	N/A	O-EME-X-ST-040621/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to sensitive information. **CVE ID : CVE-2021-27467**		
Fedoraproject					
fedora					
Exposure of Sensitive Information to an Unauthorized Actor	20-May-21	2.7	There's a flaw in Python 3's pydoc. A local or adjacent attacker who discovers or is able to convince another local or adjacent user to start a pydoc server could access the server and use it to disclose sensitive information belonging to the other user that they would not normally be able to access. The highest risk of this flaw is to data confidentiality. This flaw affects Python versions before 3.8.9, Python versions before 3.9.3 and Python versions before 3.10.0a7. **CVE ID : CVE-2021-3426**	https://bugzilla.redhat.com/show_bug.cgi?id=1935913	O-FED-FEDO-040621/503
NULL Pointer Dereference	20-May-21	5	A flaw was found in slapi-nis in versions before 0.56.7. A NULL pointer dereference during the parsing of the Binding DN could allow an unauthenticated attacker to crash the 389-ds-base directory server. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2021-3480**	https://bugzilla.redhat.com/show_bug.cgi?id=1944640	O-FED-FEDO-040621/504
Out-of-bounds Write	19-May-21	7.5	There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is able to supply a crafted file to be	https://bugzilla.redhat.com/show_bug.cgi?id=1954	O-FED-FEDO-040621/505

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
			processed by an application linked with the affected functionality of libxml2 could trigger an out-of-bounds read. The most likely impact of this flaw is to application availability, with some potential impact to confidentiality and integrity if an attacker is able to use memory information to further exploit the application. **CVE ID : CVE-2021-3517**	232	
Use After Free	18-May-21	6.8	There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by an application linked with libxml2 could trigger a use-after-free. The greatest impact from this flaw is to confidentiality, integrity, and availability. **CVE ID : CVE-2021-3518**	https://bugzilla.redhat.com/show_bug.cgi?id=1954242	O-FED-FEDO-040621/506
Improper Input Validation	17-May-21	4.3	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway) in versions before 14.2.21. The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. In addition, the prior bug fix for CVE-2020-10753 did not account for the use of \r as a header	https://bugzilla.redhat.com/show_bug.cgi?id=1951674	O-FED-FEDO-040621/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			separator, thus a new flaw has been created. **CVE ID : CVE-2021-3524**		
Improper Input Validation	18-May-21	5	A flaw was found in the Red Hat Ceph Storage RGW in versions before 14.2.21. When processing a GET Request for a swift URL that ends with two slashes it can cause the rgw to crash, resulting in a denial of service. The greatest threat to the system is of availability. **CVE ID : CVE-2021-3531**	https://bugzilla.redhat.com/show_bug.cgi?id=1955326, http://www.openwall.com/lists/oss-security/2021/05/14/5, http://www.openwall.com/lists/oss-security/2021/05/17/7	O-FED-FEDO-040621/508
IBM					
8335-gca_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-May-21	8.5	IBM Host firmware for LC-class Systems could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request that would allow them to delete arbitrary files on the system. IBM X-Force ID: 200558. **CVE ID : CVE-2021-29695**	https://www.ibm.com/support/pages/node/6454303, https://exchange.xforce.ibmcloud.com/vulnerabilities/200558	O-IBM-8335-040621/509
8335-gta_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path	25-May-21	8.5	IBM Host firmware for LC-class Systems could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request that would allow them to	https://www.ibm.com/support/pages/node/6454303, https://exchange.xforce.i	O-IBM-8335-040621/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			delete arbitrary files on the system. IBM X-Force ID: 200558. **CVE ID : CVE-2021-29695**	bmcloud.com/vulnerabilities/200558	
8335-gtb_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-May-21	8.5	IBM Host firmware for LC-class Systems could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request that would allow them to delete arbitrary files on the system. IBM X-Force ID: 200558. **CVE ID : CVE-2021-29695**	https://www.ibm.com/support/pages/node/6454303, https://exchange.xforce.ibmcloud.com/vulnerabilities/200558	O-IBM-8335-040621/511
aix					
Exposure of Sensitive Information to an Unauthorized Actor	21-May-21	5	IBM InfoSphere Information Server 11.7 could allow an attacker to obtain sensitive information by injecting parameters into an HTML query. This information could be used in further attacks against the system. IBM X-Force ID: 199918. **CVE ID : CVE-2021-29681**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199917, https://www.ibm.com/support/pages/node/6454591	O-IBM-AIX-040621/512
Generation of Error Message Containing Sensitive Information	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 199997 **CVE ID : CVE-2021-29682**	https://www.ibm.com/support/pages/node/6454587, https://exchange.xforce.ibmcloud.com/vulnerabilities/199997	O-IBM-AIX-040621/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	20-May-21	4	IBM Security Identity Manager 7.0.2 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 199998. **CVE ID : CVE-2021-29683**	https://www.ibm.com/support/pages/node/6454587, https://exchange.xforce.ibmcloud.com/vulnerabilities/199998	O-IBM-AIX-040621/514
Incorrect Permission Assignment for Critical Resource	20-May-21	6.5	IBM Security Identity Manager 7.0.2 could allow an authenticated user to bypass security and perform actions that they should not have access to. IBM X-Force ID: 200015 **CVE ID : CVE-2021-29686**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200015, https://www.ibm.com/support/pages/node/6454587	O-IBM-AIX-040621/515
Observable Discrepancy	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote user to enumerate usernames due to a difference of responses from valid and invalid login attempts. IBM X-Force ID: 200018 **CVE ID : CVE-2021-29687**	https://www.ibm.com/support/pages/node/6454605, https://exchange.xforce.ibmcloud.com/vulnerabilities/200018	O-IBM-AIX-040621/516
Generation of Error Message Containing Sensitive Information	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 200102.	https://exchange.xforce.ibmcloud.com/vulnerabilities/200102, https://www.ibm.com/support/pages/node/6454605,	O-IBM-AIX-040621/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29688	https://www.ibm.com/support/pages/node/6454587	
Use of Hard-coded Credentials	20-May-21	5	IBM Security Identity Manager 7.0.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 200252. **CVE ID : CVE-2021-29691**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200252, https://www.ibm.com/support/pages/node/6454587	O-IBM-AIX-040621/518
N/A	20-May-21	4.3	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 200253. **CVE ID : CVE-2021-29692**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200253, https://www.ibm.com/support/pages/node/6454587	O-IBM-AIX-040621/519
Improper Authentication	17-May-21	5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain highly sensitive information due to a vulnerability in the authentication mechanism. IBM X-Force ID: 201775. **CVE ID : CVE-2021-29747**	https://www.ibm.com/support/pages/node/6453437, https://exchange.xforce.ibmcloud.com/vulnerabilities/201775	O-IBM-AIX-040621/520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
intelbras					
rf_301k_firmware					
Cross-Site Request Forgery (CSRF)	17-May-21	6.8	Intelbras Router RF 301K Firmware 1.1.2 is vulnerable to Cross Site Request Forgery (CSRF) due to lack of validation and insecure configurations in inputs and modules. **CVE ID : CVE-2021-32402**	N/A	O-INT-RF_3-040621/521
Cross-Site Request Forgery (CSRF)	17-May-21	6.8	Intelbras Router RF 301K Firmware 1.1.2 is vulnerable to Cross Site Request Forgery (CSRF) due to lack of security mechanisms for token protection and unsafe inputs and modules. **CVE ID : CVE-2021-32403**	N/A	O-INT-RF_3-040621/522
Linux					
linux_kernel					
Insufficiently Protected Credentials	24-May-21	2.1	IBM Security Guardium 11.2 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 195770. **CVE ID : CVE-2021-20389**	https://www.ibm.com/support/pages/node/6455281, https://exchange.xforce.ibmcloud.com/vulnerabilities/195770	O-LIN-LINU-040621/523
Use of a Broken or Risky Cryptographic Algorithm	24-May-21	5	IBM Security Guardium 11.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 196280. **CVE ID : CVE-2021-20419**	https://www.ibm.com/support/pages/node/6455281, https://exchange.xforce.ibmcloud.com	O-LIN-LINU-040621/524

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
				/vulnerabilities/196280	
Use of Hard-coded Credentials	24-May-21	7.5	IBM Security Guardium 11.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 196313. **CVE ID : CVE-2021-20426**	https://www.ibm.com/support/pages/node/6455281, https://exchange.xforce.ibmcloud.com/vulnerabilities/196313	O-LIN-LINU-040621/525
Generation of Error Message Containing Sensitive Information	24-May-21	5	IBM Security Guardium 11.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196315. **CVE ID : CVE-2021-20428**	https://www.ibm.com/support/pages/node/6455281, https://exchange.xforce.ibmcloud.com/vulnerabilities/196315	O-LIN-LINU-040621/526
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-May-21	9	IBM Security Guardium 11.2 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 199184. **CVE ID : CVE-2021-20557**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199184, https://www.ibm.com/support/pages/node/6455269	O-LIN-LINU-040621/527
Exposure of Sensitive Information to an Unauthorize	21-May-21	5	IBM InfoSphere Information Server 11.7 could allow an attacker to obtain sensitive information by injecting parameters into an HTML	https://exchange.xforce.ibmcloud.com/vulnerabilities/199917,	O-LIN-LINU-040621/528

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
d Actor			query. This information could be used in further attacks against the system. IBM X-Force ID: 199918. **CVE ID : CVE-2021-29681**	https://www.ibm.com/support/pages/node/6454591	
Generation of Error Message Containing Sensitive Information	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 199997 **CVE ID : CVE-2021-29682**	https://www.ibm.com/support/pages/node/6454587, https://exchange.xforce.ibmcloud.com/vulnerabilities/199997	O-LIN-LINU-040621/529
Cleartext Storage of Sensitive Information	20-May-21	4	IBM Security Identity Manager 7.0.2 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 199998. **CVE ID : CVE-2021-29683**	https://www.ibm.com/support/pages/node/6454587, https://exchange.xforce.ibmcloud.com/vulnerabilities/199998	O-LIN-LINU-040621/530
Incorrect Permission Assignment for Critical Resource	20-May-21	6.5	IBM Security Identity Manager 7.0.2 could allow an authenticated user to bypass security and perform actions that they should not have access to. IBM X-Force ID: 200015 **CVE ID : CVE-2021-29686**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200015, https://www.ibm.com/support/pages/node/6454587	O-LIN-LINU-040621/531
Observable Discrepancy	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote user to enumerate usernames	https://www.ibm.com/support/page	O-LIN-LINU-040621/532

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
			due to a difference of responses from valid and invalid login attempts. IBM X-Force ID: 200018 **CVE ID : CVE-2021-29687**	s/node/6454605, https://exchange.xforce.ibmcloud.com/vulnerabilities/200018	
Generation of Error Message Containing Sensitive Information	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 200102. **CVE ID : CVE-2021-29688**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200102, https://www.ibm.com/support/pages/node/6454605, https://www.ibm.com/support/pages/node/6454587	O-LIN-LINU-040621/533
Use of Hard-coded Credentials	20-May-21	5	IBM Security Identity Manager 7.0.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 200252. **CVE ID : CVE-2021-29691**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200252, https://www.ibm.com/support/pages/node/6454587	O-LIN-LINU-040621/534
N/A	20-May-21	4.3	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could	https://exchange.xforce.ibmcloud.com/vulnerabilities/200253, https://www.ibm.com/s	O-LIN-LINU-040621/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 200253. **CVE ID : CVE-2021-29692**	upport/pages/node/6454587	
Improper Authentication	17-May-21	5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain highly sensitive information due to a vulnerability in the authentication mechanism. IBM X-Force ID: 201775. **CVE ID : CVE-2021-29747**	https://www.ibm.com/support/pages/node/6453437, https://exchange.xforce.ibmcloud.com/vulnerabilities/201775	O-LIN-LINU-040621/536
Incorrect Calculation	21-May-21	6.9	This vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel 5.11.15. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of eBPF programs. The issue results from the lack of proper validation of user-supplied eBPF programs prior to executing them. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel. Was ZDI-CAN-13661. **CVE ID : CVE-2021-31440**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=10bf4e83167cc68595b85fd73bb91e8f2c086e36	O-LIN-LINU-040621/537
Use After Free	17-May-21	4.6	A flaw was found in the Nosy driver in the Linux kernel. This issue allows a device to	http://www.openwall.com/lists/oss-	O-LIN-LINU-040621/538

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
			be inserted twice into a doubly-linked list, leading to a use-after-free when one of these devices is removed. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. Versions before kernel 5.12-rc6 are affected **CVE ID : CVE-2021-3483**	security/2021/04/07/1, https://bugzilla.redhat.com/show_bug.cgi?id=1948045	
Microsoft					
windows					
Improper Control of Generation of Code ('Code Injection')	18-May-21	4.6	RabbitMQ installers on Windows prior to version 3.8.16 do not harden plugin directory permissions, potentially allowing attackers with sufficient local filesystem permissions to add arbitrary plugins. **CVE ID : CVE-2021-22117**	https://tanzu.vmware.com/security/cve-2021-22117	O-MIC-WIND-040621/539
Exposure of Sensitive Information to an Unauthorized Actor	21-May-21	5	IBM InfoSphere Information Server 11.7 could allow an attacker to obtain sensitive information by injecting parameters into an HTML query. This information could be used in further attacks against the system. IBM X-Force ID: 199918. **CVE ID : CVE-2021-29681**	https://exchange.xforce.ibmcloud.com/vulnerabilities/199917, https://www.ibm.com/support/pages/node/6454591	O-MIC-WIND-040621/540
Generation of Error Message Containing Sensitive Information	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in	https://www.ibm.com/support/pages/node/6454587, https://exchange.xforce.i	O-MIC-WIND-040621/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			further attacks against the system. IBM X-Force ID: 199997 **CVE ID : CVE-2021-29682**	bmcloud.com/vulnerabilities/199997	
Cleartext Storage of Sensitive Information	20-May-21	4	IBM Security Identity Manager 7.0.2 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 199998. **CVE ID : CVE-2021-29683**	https://www.ibm.com/support/pages/node/6454587, https://exchange.xforce.ibmcloud.com/vulnerabilities/199998	O-MIC-WIND-040621/542
Incorrect Permission Assignment for Critical Resource	20-May-21	6.5	IBM Security Identity Manager 7.0.2 could allow an authenticated user to bypass security and perform actions that they should not have access to. IBM X-Force ID: 200015 **CVE ID : CVE-2021-29686**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200015, https://www.ibm.com/support/pages/node/6454587	O-MIC-WIND-040621/543
Observable Discrepancy	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote user to enumerate usernames due to a difference of responses from valid and invalid login attempts. IBM X-Force ID: 200018 **CVE ID : CVE-2021-29687**	https://www.ibm.com/support/pages/node/6454605, https://exchange.xforce.ibmcloud.com/vulnerabilities/200018	O-MIC-WIND-040621/544
Generation of Error Message Containing Sensitive	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This	https://exchange.xforce.ibmcloud.com/vulnerabilities/200102, https://ww	O-MIC-WIND-040621/545

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
Information			information could be used in further attacks against the system. IBM X-Force ID: 200102. **CVE ID : CVE-2021-29688**	w.ibm.com/support/pages/node/6454605, https://www.ibm.com/support/pages/node/6454587	
Use of Hard-coded Credentials	20-May-21	5	IBM Security Identity Manager 7.0.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 200252. **CVE ID : CVE-2021-29691**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200252, https://www.ibm.com/support/pages/node/6454587	O-MIC-WIND-040621/546
N/A	20-May-21	4.3	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 200253. **CVE ID : CVE-2021-29692**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200253, https://www.ibm.com/support/pages/node/6454587	O-MIC-WIND-040621/547
Improper Authentication	17-May-21	5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain highly sensitive information due to a vulnerability in the authentication mechanism.	https://www.ibm.com/support/pages/node/6453437, https://exchange.xforce.i	O-MIC-WIND-040621/548

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
			IBM X-Force ID: 201775. **CVE ID : CVE-2021-29747**	bmcloud.com/vulnerabilities/201775	
Out-of-bounds Write	21-May-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the browseForDoc function. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13523. **CVE ID : CVE-2021-31473**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-040621/549
N/A	21-May-21	5	PuTTY before 0.75 on Windows allows remote servers to cause a denial of service (Windows GUI hang) by telling the PuTTY window to change its title repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls. NOTE: the same attack methodology may affect some OS-level GUIs on Linux or other platforms for similar reasons. **CVE ID : CVE-2021-33500**	N/A	O-MIC-WIND-040621/550

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
Netgear					
gc108pp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-GC10-040621/551
gc108p_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authenticati	O-NET-GC10-040621/552

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
Command Injection')			demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	on-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	
gs108t_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-GS10-040621/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
gs110tpp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-GS11-040621/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
gs110tp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-GS11-040621/555
gs110tup_firmware					
Improper Neutralizatio	21-May-21	10	Certain NETGEAR devices are affected by command	https://kb.netgear.com/0	O-NET-GS11-040621/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	00063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	
gs710tup_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability	O-NET-GS71-040621/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	-on-Some-Smart-Switches-PSV-2021-0071	
gs716tpp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-GS71-040621/558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
gs716tp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3.	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-GS71-040621/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33514		
gs724tpp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-GS72-040621/560
gs724tp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authenticati	O-NET-GS72-040621/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	on-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	
gs728tpp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-GS72-040621/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
gs728tp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-GS72-040621/563

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
			before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
gs752tpp_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-GS75-040621/564
gs752tp_firmware					
Improper Neutralizatio	21-May-21	10	Certain NETGEAR devices are affected by command	https://kb.netgear.com/0	O-NET-GS75-040621/565

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
n of Special Elements used in an OS Command ('OS Command Injection')			injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	00063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	
ms510txm_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability	O-NET-MS51-040621/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**	-on-Some-Smart-Switches-PSV-2021-0071	
ms510txup_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-May-21	10	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker via the vulnerable /sqfs/lib/libsal.so.0.0 library used by a CGI application, as demonstrated by setup.cgi?token=';$HTTP_USER_AGENT;' with an OS command in the User-Agent field. This affects GC108P before 1.0.7.3, GC108PP before 1.0.7.3, GS108Tv3 before 7.0.6.3, GS110TPPv1 before 7.0.6.3, GS110TPv3 before 7.0.6.3, GS110TUPv1 before 1.0.4.3, GS710TUPv1 before 1.0.4.3, GS716TP before 1.0.2.3, GS716TPP	https://kb.netgear.com/000063641/Security-Advisory-for-Pre-Authentication-Command-Injection-Vulnerability-on-Some-Smart-Switches-PSV-2021-0071	O-NET-MS51-040621/567

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
			before 1.0.2.3, GS724TPPv1 before 2.0.4.3, GS724TPv2 before 2.0.4.3, GS728TPPv2 before 6.0.6.3, GS728TPv2 before 6.0.6.3, GS752TPPv1 before 6.0.6.3, GS752TPv2 before 6.0.6.3, MS510TXM before 1.0.2.3, and MS510TXUP before 1.0.2.3. **CVE ID : CVE-2021-33514**		
nippon-antenna					
rfntps_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-May-21	7.7	RFNTPS firmware versions System_01000004 and earlier, and Web_01000004 and earlier allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors. **CVE ID : CVE-2021-20719**	https://www.nippon-antenna.co.jp/ja/news/news/news8217702780390204428.html	O-NIP-RFNT-040621/568
Oracle					
solaris					
Generation of Error Message Containing Sensitive Information	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 199997 **CVE ID : CVE-2021-29682**	https://www.ibm.com/support/pages/node/6454587, https://exchange.xforce.ibmcloud.com/vulnerabilities/199997	O-ORA-SOLA-040621/569
Cleartext Storage of Sensitive	20-May-21	4	IBM Security Identity Manager 7.0.2 stores user credentials in plain clear text which can be	https://www.ibm.com/support/page	O-ORA-SOLA-040621/570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			read by an authenticated user. IBM X-Force ID: 199998. **CVE ID : CVE-2021-29683**	s/node/6454587, https://exchange.xforce.ibmcloud.com/vulnerabilities/199998	
Incorrect Permission Assignment for Critical Resource	20-May-21	6.5	IBM Security Identity Manager 7.0.2 could allow an authenticated user to bypass security and perform actions that they should not have access to. IBM X-Force ID: 200015 **CVE ID : CVE-2021-29686**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200015, https://www.ibm.com/support/pages/node/6454587	O-ORA-SOLA-040621/571
Observable Discrepancy	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote user to enumerate usernames due to a difference of responses from valid and invalid login attempts. IBM X-Force ID: 200018 **CVE ID : CVE-2021-29687**	https://www.ibm.com/support/pages/node/6454605, https://exchange.xforce.ibmcloud.com/vulnerabilities/200018	O-ORA-SOLA-040621/572
Generation of Error Message Containing Sensitive Information	20-May-21	5	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 200102. **CVE ID : CVE-2021-29688**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200102, https://www.ibm.com/support/pages/node/6454605, https://www.ibm.com/support/page	O-ORA-SOLA-040621/573

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
				s/node/6454587	
Use of Hard-coded Credentials	20-May-21	5	IBM Security Identity Manager 7.0.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 200252. **CVE ID : CVE-2021-29691**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200252, https://www.ibm.com/support/pages/node/6454587	O-ORA-SOLA-040621/574
N/A	20-May-21	4.3	IBM Security Identity Manager 7.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 200253. **CVE ID : CVE-2021-29692**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200253, https://www.ibm.com/support/pages/node/6454587	O-ORA-SOLA-040621/575
Redhat					
enterprise_linux					
Exposure of Sensitive Information to an Unauthorized Actor	20-May-21	2.7	There's a flaw in Python 3's pydoc. A local or adjacent attacker who discovers or is able to convince another local or adjacent user to start a pydoc server could access the server and use it to disclose sensitive information belonging to the other user that they would not normally be able to access. The highest	https://bugzilla.redhat.com/show_bug.cgi?id=1935913	O-RED-ENTE-040621/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			risk of this flaw is to data confidentiality. This flaw affects Python versions before 3.8.9, Python versions before 3.9.3 and Python versions before 3.10.0a7. **CVE ID : CVE-2021-3426**		
Out-of-bounds Write	19-May-21	7.5	There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is able to supply a crafted file to be processed by an application linked with the affected functionality of libxml2 could trigger an out-of-bounds read. The most likely impact of this flaw is to application availability, with some potential impact to confidentiality and integrity if an attacker is able to use memory information to further exploit the application. **CVE ID : CVE-2021-3517**	https://bugzilla.redhat.com/show_bug.cgi?id=1954232	O-RED-ENTE-040621/577
Use After Free	18-May-21	6.8	There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by an application linked with libxml2 could trigger a use-after-free. The greatest impact from this flaw is to confidentiality, integrity, and availability. **CVE ID : CVE-2021-3518**	https://bugzilla.redhat.com/show_bug.cgi?id=1954242	O-RED-ENTE-040621/578
sitel-sa					
cap\\/prx_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	17-May-21	2.1	SITEL CAP/PRX firmware version 5.2.01 allows an attacker with access to the local network, to access via HTTP to the internal configuration database of the device without any authentication. An attacker could exploit this vulnerability in order to obtain information about the device´s configuration. **CVE ID : CVE-2021-32453**	https://www.incibe-cert.es/en/early-warning/ics-advisories/sitel-capprx-information-exposure	O-SIT-CAP\-040621/579
Uncontrolled Resource Consumption	17-May-21	6.1	SITEL CAP/PRX firmware version 5.2.01, allows an attacker with access to the device´s network to cause a denial of service condition on the device. An attacker could exploit this vulnerability by sending HTTP requests massively. **CVE ID : CVE-2021-32455**	https://www.incibe-cert.es/en/early-warning/ics-advisories/sitel-capprx-vulnerable-denial-service-attack	O-SIT-CAP\-040621/580
remote_cap\\/prx_firmware					
Use of Hard-coded Credentials	17-May-21	5.8	SITEL CAP/PRX firmware version 5.2.01 makes use of a hardcoded password. An attacker with access to the device could modify these credentials, leaving the administrators of the device without access. **CVE ID : CVE-2021-32454**	https://www.incibe-cert.es/en/early-warning/ics-advisories/sitel-capprx-hardcoded-credentials	O-SIT-REMO-040621/581
Cleartext Transmission of Sensitive Information	17-May-21	3.3	SITEL CAP/PRX firmware version 5.2.01 allows an attacker with access to the local network of the device to obtain the authentication	https://www.incibe-cert.es/en/early-warning/ics-	O-SIT-REMO-040621/582

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
			passwords by analysing the network traffic. **CVE ID : CVE-2021-32456**	advisories/sitel-capprx-cleartext-transmission-sensitive-information	
Wago					
750-8202_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/583
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/584
750-8203_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/585
Improper Limitation of a Pathname	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets	https://cert.vde.com/en-us/advisorie	O-WAG-750--040621/586

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
to a Restricted Directory ('Path Traversal')			an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	s/vde-2021-014	
750-8204_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/587
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/588
750-8206_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/589
Improper Limitation of a Pathname to a Restricted	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/590

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
Directory ('Path Traversal')			can access the file system with higher privileges. **CVE ID : CVE-2021-21001**		
750-8207_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/591
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/592
750-8208_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/593
Improper Limitation of a Pathname to a Restricted Directory ('Path	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges.	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			**CVE ID : CVE-2021-21001**		
750-8210_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/595
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/596
750-8211_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/597
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/598

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
750-8212_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/599
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/600
750-8213_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/601
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/602
750-8214_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/603
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/604
750-8216_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/605
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/606
750-8217_firmware					
Allocation of Resources	24-May-21	5	On WAGO PFC200 devices in different firmware versions	https://cert.vde.com/en-	O-WAG-750--040621/607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	us/advisories/vde-2021-014	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/608
750-823_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/609
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/610
750-829_firmware					
Allocation of Resources Without Limits or	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network	https://cert.vde.com/en-us/advisories/vde-2021-	O-WAG-750--040621/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Throttling			access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	014	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/612
750-831_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/613
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/614
750-832_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the login service of the runtime. **CVE ID : CVE-2021-21000**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/616
750-852_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/617
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/618
750-862_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime.	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21000		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/620
750-880_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/621
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/622
750-881_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/624
750-882_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/625
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/626
750-885_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/627
Improper Limitation of	24-May-21	4	On WAGO PFC200 devices in different firmware versions	https://cert.vde.com/en-	O-WAG-750--040621/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	us/advisories/vde-2021-014	
750-889_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/629
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/630
750-890_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/631
Improper Limitation of a Pathname to a	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with	https://cert.vde.com/en-us/advisories/vde-2021-	O-WAG-750--040621/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	014	
750-891_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/633
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with higher privileges. **CVE ID : CVE-2021-21001**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/634
750-893_firmware					
Allocation of Resources Without Limits or Throttling	24-May-21	5	On WAGO PFC200 devices in different firmware versions with special crafted packets an attacker with network access to the device could cause a denial of service for the login service of the runtime. **CVE ID : CVE-2021-21000**	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/635
Improper Limitation of a Pathname to a Restricted Directory	24-May-21	4	On WAGO PFC200 devices in different firmware versions with special crafted packets an authorised attacker with network access to the device can access the file system with	https://cert.vde.com/en-us/advisories/vde-2021-014	O-WAG-750--040621/636

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
('Path Traversal')			higher privileges. **CVE ID : CVE-2021-21001**		
zephyrproject					
zephyr					
NULL Pointer Dereference	25-May-21	5	Type Confusion in 802154 ACK Frames Handling. Zephyr versions >= v2.4.0 contain NULL Pointer Dereference (CWE-476). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-27r3-rxch-2hm7 **CVE ID : CVE-2021-3320**	N/A	O-ZEP-ZEPH-040621/637
ZTE					
axon_11_5g_firmware					
Incorrect Default Permissions	19-May-21	5	A mobile phone of ZTE is impacted by improper access control vulnerability. Due to improper permission settings, third-party applications can read some files in the proc file system without authorization. Attackers could exploit this vulnerability to obtain sensitive information. This affects Axon 11 5G ZTE/CN_P725A12/P725A12:10/QKQ1.200816.002/20201116.175317:user/release-keys. **CVE ID : CVE-2021-21732**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1015064	O-ZTE-AXON-040621/638