National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Aug 2021 Vol. 08 No. 15

https://nciipc.gov.in

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
aapanel					
aapanel					
N/A	02-Aug-21	6.8	aaPanel through 6.8.12 allows Cross-Site WebSocket Hijacking (CSWH) involving OS commands within WebSocket messages at a ws:// URL for /webssh (the victim must have configured Terminal with at least one host). Successful exploitation depends on the browser used by a potential victim (e.g., exploitation can occur with Firefox but not Chrome). **CVE ID : CVE-2021-37840**	N/A	A-AAP-AAPA-180821/1
Acronis					
cyber_protection_agent					
Improper Certificate Validation	05-Aug-21	5.8	Acronis True Image prior to 2021 Update 4 for Windows, Acronis True Image prior to 2021 Update 5 for Mac, Acronis Agent prior to build 26653, Acronis Cyber Protect prior to build 27009 did not implement SSL certificate validation. **CVE ID : CVE-2021-32581**	https://kb.acronis.com/content/68413, https://kb.acronis.com/content/68419, https://kb.acronis.com/content/68648	A-ACR-CYBE-180821/2
cyber_protect_cloud					
Improper Certificate	05-Aug-21	5.8	Acronis True Image prior to 2021 Update 4 for Windows,	https://kb.acronis.com/co	A-ACR-CYBE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Acronis True Image prior to 2021 Update 5 for Mac, Acronis Agent prior to build 26653, Acronis Cyber Protect prior to build 27009 did not implement SSL certificate validation. **CVE ID : CVE-2021-32581**	ntent/68413, https://kb.acronis.com/content/68419, https://kb.acronis.com/content/68648	180821/3
true_image					
Externally Controlled Reference to a Resource in Another Sphere	05-Aug-21	4.6	Acronis True Image prior to 2021 Update 4 for Windows allowed local privilege escalation due to improper soft link handling (issue 1 of 2). **CVE ID : CVE-2021-32576**	https://kb.acronis.com/content/68419	A-ACR-TRUE-180821/4
Improper Privilege Management	05-Aug-21	4.6	Acronis True Image prior to 2021 Update 5 for Windows allowed local privilege escalation due to insecure folder permissions. **CVE ID : CVE-2021-32577**	https://kb.acronis.com/content/68413	A-ACR-TRUE-180821/5
Externally Controlled Reference to a Resource in Another Sphere	05-Aug-21	4.6	Acronis True Image prior to 2021 Update 4 for Windows allowed local privilege escalation due to improper soft link handling (issue 2 of 2). **CVE ID : CVE-2021-32578**	https://kb.acronis.com/content/68419	A-ACR-TRUE-180821/6
Improper Authentication	05-Aug-21	4.6	Acronis True Image prior to 2021 Update 4 for Windows and Acronis True Image prior to 2021 Update 5 for macOS allowed an unauthenticated attacker (who has a local code execution ability) to tamper	https://kb.acronis.com/content/68413, https://kb.acronis.com/content/68419	A-ACR-TRUE-180821/7

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with the micro-service API. **CVE ID : CVE-2021-32579**		
Uncontrolled Search Path Element	05-Aug-21	4.4	Acronis True Image prior to 2021 Update 4 for Windows allowed local privilege escalation due to DLL hijacking. **CVE ID : CVE-2021-32580**	https://kb.acronis.com/content/68419	A-ACR-TRUE-180821/8
Improper Certificate Validation	05-Aug-21	5.8	Acronis True Image prior to 2021 Update 4 for Windows, Acronis True Image prior to 2021 Update 5 for Mac, Acronis Agent prior to build 26653, Acronis Cyber Protect prior to build 27009 did not implement SSL certificate validation. **CVE ID : CVE-2021-32581**	https://kb.acronis.com/content/68413, https://kb.acronis.com/content/68419, https://kb.acronis.com/content/68648	A-ACR-TRUE-180821/9
Advantech					
r-seenet					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-21	10	An OS Command Injection vulnerability exists in the ping.php script functionality of Advantech R-SeeNet v 2.4.12 (20.10.2020). A specially crafted HTTP request can lead to arbitrary OS command execution. An attacker can send a crafted HTTP request to trigger this vulnerability. **CVE ID : CVE-2021-21805**	N/A	A-ADV-R-SE-180821/10
akaunting					
akaunting					
Improper Control of	04-Aug-21	9	Akaunting version 2.1.12 and earlier suffers from a code	N/A	A-AKA-AKAU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			injection issue in the Money.php component of the application. A POST sent to /{company_id}/sales/invoices /{invoice_id} with an items[0][price] that includes a PHP callable function is executed directly. This issue was fixed in version 2.1.13 of the product. **CVE ID : CVE-2021-36800**		180821/11
Authorization Bypass Through User-Controlled Key	04-Aug-21	5.5	Akaunting version 2.1.12 and earlier suffers from an authentication bypass issue in the user-controllable field, companies[0]. This issue was fixed in version 2.1.13 of the product. **CVE ID : CVE-2021-36801**	N/A	A-AKA-AKAU-180821/12
N/A	04-Aug-21	4	Akaunting version 2.1.12 and earlier suffers from a denial-of-service issue that is triggered by setting a malformed 'locale' variable and sending it in an otherwise normal HTTP POST request. This issue was fixed in version 2.1.13 of the product. **CVE ID : CVE-2021-36802**	N/A	A-AKA-AKAU-180821/13
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	3.5	Akaunting version 2.1.12 and earlier suffers from a persistent (type II) cross-site scripting (XSS) vulnerability in processing user-supplied avatar images. This issue was fixed in version 2.1.13 of the product.	N/A	A-AKA-AKAU-180821/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36803		
Weak Password Recovery Mechanism for Forgotten Password	04-Aug-21	5.8	Akaunting version 2.1.12 and earlier suffers from a password reset spoofing vulnerability, wherein an attacker can proxy password reset requests through a running Akaunting instance, if that attacker knows the target's e-mail address. This issue was fixed in version 2.1.13 of the product. Please note that this issue is ultimately caused by the defaults provided by the Laravel framework, specifically how proxy headers are handled with respect to multi-tenant implementations. In other words, while this is not technically a vulnerability in Laravel, this default configuration is very likely to lead to practically identical identical vulnerabilities in Laravel projects that implement multi-tenant applications. **CVE ID : CVE-2021-36804**	https://github.com/laravel/laravel/pull/5477	A-AKA-AKAU-180821/15
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	3.5	Akaunting version 2.1.12 and earlier suffers from a persistent (type II) cross-site scripting (XSS) vulnerability in the sales invoice processing component of the application. This issue was fixed in version 2.1.13 of the product.	N/A	A-AKA-AKAU-180821/16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36805		
any_hostname_project					
any_hostname					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The Any Hostname WordPress plugin through 1.0.6 does not sanitise or escape its "Allowed hosts" setting, leading to an authenticated stored XSS issue as high privilege users are able to set XSS payloads in it **CVE ID : CVE-2021-24481**	N/A	A-ANY-ANY_-180821/17
argo-workflows_project					
argo-workflows					
Improper Input Validation	03-Aug-21	5.8	In Argo Workflows through 3.1.3, if EXPRESSION_TEMPLATES is enabled and untrusted users are allowed to specify input parameters when running workflows, an attacker may be able to disrupt a workflow because expression template output is evaluated. **CVE ID : CVE-2021-37914**	https://github.com/argoproj/argo-workflows/pull/6442	A-ARG-ARGO-180821/18
Atlassian					
confluence					
Missing Authorization	03-Aug-21	5	Affected versions of Atlassian Confluence Server allow remote attackers to view restricted resources via a Pre-Authorization Arbitrary File Read vulnerability in the /s/ endpoint. The affected versions are before version	https://jira.atlassian.com/browse/CONFSERVER-67893	A-ATL-CONF-180821/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.4.10, and from version 7.5.0 before 7.12.3. **CVE ID : CVE-2021-26085**		
saml_single_sign_on					
Missing Authentication for Critical Function	02-Aug-21	7.5	The resolution SAML SSO apps for Atlassian products allow a remote attacker to login to a user account when only the username is known (i.e., no other authentication is provided). The fixed versions are for Jira: 3.6.6.1, 4.0.12, 5.0.5; for Confluence 3.6.6, 4.0.12, 5.0.5; for Bitbucket 2.5.9, 3.6.6, 4.0.12, 5.0.5; for Bamboo 2.5.9, 3.6.6, 4.0.12, 5.0.5; and for Fisheye 2.5.9. **CVE ID : CVE-2021-37843**	N/A	A-ATL-SAML-180821/20
atomicparsley_project					
atomicparsley					
Out-of-bounds Write	04-Aug-21	4.3	A stack-buffer-overflow occurs in Atomicparsley 20210124.204813.840499f through APar_readX() in src/util.cpp while parsing a crafted mp4 file because of the missing boundary check. **CVE ID : CVE-2021-37231**	https://github.com/wez/atomicparsley/issues/30	A-ATO-ATOM-180821/21
Out-of-bounds Write	04-Aug-21	7.5	A stack overflow vulnerability occurs in Atomicparsley 20210124.204813.840499f through APar_read64() in src/util.cpp due to the lack of buffer size of uint32_buffer while reading more bytes in	https://github.com/wez/atomicparsley/issues/32, https://github.com/wez/atomicparsley/commit/d7	A-ATO-ATOM-180821/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APar_read64. **CVE ID : CVE-2021-37232**	2ccf06c9825 9d7261e0f3a c4fd8717778 782c1	
awesome_weather_widget					
awesome_weather_widget					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	4.3	The Awesome Weather Widget WordPress plugin through 3.0.2 does not sanitize the id parameter of its awesome_weather_refresh AJAX action, leading to an unauthenticated Reflected Cross-Site Scripting (XSS) Vulnerability. **CVE ID : CVE-2021-24474**	N/A	A-AWE-AWES-180821/23
axiosys					
bento4					
NULL Pointer Dereference	05-Aug-21	4.3	An issue was discovered in Bento4 through v1.6.0-636. A NULL pointer dereference exists in the function AP4_StszAtom::WriteFields located in Ap4StszAtom.cpp. It allows an attacker to cause a denial of service (DOS). **CVE ID : CVE-2021-35306**	N/A	A-AXI-BENT-180821/24
NULL Pointer Dereference	05-Aug-21	4.3	An issue was discovered in Bento4 through v1.6.0-636. A NULL pointer dereference exists in the AP4_DescriptorFinder::Test component located in /Core/Ap4Descriptor.h. It allows an attacker to cause a denial of service (DOS).	N/A	A-AXI-BENT-180821/25

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-35307		
ays-pro					
faq_builder					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-21	6.5	The get_faqs() function in the FAQ Builder AYS WordPress plugin before 1.3.6 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the get_results() DB calls, leading to SQL injection issues in the admin dashboard **CVE ID : CVE-2021-24461**	N/A	A-AYS-FAQ_-180821/26
image_slider					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-21	6.5	The get_sliders() function in the Image Slider by Ays-Responsive Slider and Carousel WordPress plugin before 2.5.0 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the get_results() DB calls, leading to SQL injection issues in the admin dashboard **CVE ID : CVE-2021-24463**	N/A	A-AYS-IMAG-180821/27
photo_gallery					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-21	6.5	The get_gallery_categories() and get_galleries() functions in the Photo Gallery by Ays â€“ Responsive Image Gallery WordPress plugin before 4.4.4 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the get_results() DB calls, leading	N/A	A-AYS-PHOT-180821/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to SQL injection issues in the admin dashboard **CVE ID : CVE-2021-24462**		
poll_maker					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-21	6.5	The get_poll_categories(), get_polls() and get_reports() functions in the Poll Maker WordPress plugin before 3.2.1 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the get_results() DB calls, leading to SQL injection issues in the admin dashboard **CVE ID : CVE-2021-24483**	N/A	A-AYS-POLL-180821/29
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	4.3	The Poll Maker WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the mcount parameter found in the ~/admin/partials/settings/poll-maker-settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.2.8. **CVE ID : CVE-2021-34635**	N/A	A-AYS-POLL-180821/30
popup_box					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	02-Aug-21	6.5	The get_ays_popupboxes() and get_popup_categories() functions of the Popup box WordPress plugin before 2.3.4 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the	N/A	A-AYS-POPU-180821/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			get_results() DB calls, leading to SQL injection issues in the admin dashboard **CVE ID : CVE-2021-24458**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-21	6.5	The get_fb_likeboxes() function in the Popup Like box â€“ Page Plugin WordPress plugin before 3.5.3 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the get_results() DB calls, leading to SQL injection issues in the admin dashboard **CVE ID : CVE-2021-24460**	N/A	A-AYS-POPU-180821/32
portfolio_responsive_gallery					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-21	6.5	The get_portfolios() and get_portfolio_attributes() functions in the class-portfolio-responsive-gallery-list-table.php and class-portfolio-responsive-gallery-attributes-list-table.php files of the Portfolio Responsive Gallery WordPress plugin before 1.1.8 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the get_results() DB calls, leading to SQL injection issues in the admin dashboard **CVE ID : CVE-2021-24457**	N/A	A-AYS-PORT-180821/33
quiz_maker					
Improper Neutralizatio	02-Aug-21	6.5	The Quiz Maker WordPress plugin before 6.2.0.9 did not	N/A	A-AYS-QUIZ-180821/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			properly sanitise and escape the order and orderby parameters before using them in SQL statements, leading to SQL injection issues in the admin dashboard **CVE ID : CVE-2021-24456**		
secure_copy_content_protection_and_content_locking					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-21	6.5	The get_reports() function in the Secure Copy Content Protection and Content Locking WordPress plugin before 2.6.7 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the get_results() DB calls, leading to SQL injection issues in the admin dashboard **CVE ID : CVE-2021-24484**	N/A	A-AYS-SECU-180821/35
survey_maker					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-21	6.5	The get_results() and get_items() functions in the Survey Maker WordPress plugin before 1.5.6 did not use whitelist or validate the orderby parameter before using it in SQL statements passed to the get_results() DB calls, leading to SQL injection issues in the admin dashboard **CVE ID : CVE-2021-24459**	N/A	A-AYS-SURV-180821/36
b2x_project					
b2x					
Incorrect Authorizatio	03-Aug-21	5	A security flaw in the 'owned' function of a smart contract	N/A	A-B2X-B2X-180821/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			implementation for BTC2X (B2X), a tradeable Ethereum ERC20 token, allows attackers to hijack victim accounts and arbitrarily increase the digital supply of assets. **CVE ID : CVE-2021-34273**		
bookshelf_project					
bookshelf					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The Bookshelf WordPress plugin through 2.0.4 does not sanitise or escape its "Paypal email address" setting before outputting it in the page, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24478**	N/A	A-BOO-BOOK-180821/38
bozdoz					
leaflet_map					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The Leaflet Map WordPress plugin before 3.0.0 does not escape some shortcode attributes before they are used in JavaScript code or HTML, which could allow users with a role as low as Contributors to exploit stored XSS issues **CVE ID : CVE-2021-24468**	N/A	A-BOZ-LEAF-180821/39
Care2x					
hospital_information_management_system					
Improper Neutralization of Special Elements	06-Aug-21	7.5	SQL Injection Vulnerability in Care2x Open Source Hospital Information Management 2.7 Alpha via the (1) pday, (2)	N/A	A-CAR-HOSP-180821/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			pmonth, and (3) pyear parameters in GET requests sent to /modules/nursing/nursing-station.php. **CVE ID : CVE-2021-36351**		
Centreon					
centreon					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-21	6.5	A SQL injection vulnerability in reporting export in Centreon before 20.04.14, 20.10.8, and 21.04.2 allows remote authenticated (but low-privileged) attackers to execute arbitrary SQL commands via the include/reporting/dashboard/csvExport/csv_HostGroupLogs.php start and end parameters. **CVE ID : CVE-2021-37556**	https://github.com/centreon/centreon/pull/9781	A-CEN-CENT-180821/41
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-21	6.5	A SQL injection vulnerability in image generation in Centreon before 20.04.14, 20.10.8, and 21.04.2 allows remote authenticated (but low-privileged) attackers to execute arbitrary SQL commands via the include/views/graphs/generateGraphs/generateImage.php index parameter. **CVE ID : CVE-2021-37557**	https://github.com/centreon/centreon/pull/9787	A-CEN-CENT-180821/42
Improper Neutralization of Special Elements	03-Aug-21	7.5	A SQL injection vulnerability in a MediaWiki script in Centreon before 20.04.14, 20.10.8, and 21.04.2 allows	https://github.com/centreon/centreon/pull/9796	A-CEN-CENT-180821/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			remote unauthenticated attackers to execute arbitrary SQL commands via the host_name and service_description parameters. The vulnerability can be exploited only when a valid Knowledge Base URL is configured on the Knowledge Base configuration page and points to a MediaWiki instance. This relates to the proxy feature in class/centreon-knowledge/ProceduresProxy.class.php and include/configuration/configKnowledge/proxy/proxy.php. **CVE ID : CVE-2021-37558**		
chikitsa					
patient_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-21	3.5	index.php/admin/add_user in Chikitsa Patient Management System 2.0.0 allows XSS. **CVE ID : CVE-2021-38149**	N/A	A-CHI-PATI-180821/44
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-21	3.5	index.php/appointment/todos in Chikitsa Patient Management System 2.0.0 allows XSS. **CVE ID : CVE-2021-38151**	N/A	A-CHI-PATI-180821/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-21	3.5	index.php/appointment/insert_patient_add_appointment in Chikitsa Patient Management System 2.0.0 allows XSS. **CVE ID : CVE-2021-38152**	N/A	A-CHI-PATI-180821/46
Cisco					
confd					
Improper Privilege Management	04-Aug-21	6.9	A vulnerability in ConfD could allow an authenticated, local attacker to execute arbitrary commands at the level of the account under which ConfD is running, which is commonly root. To exploit this vulnerability, an attacker must have a valid account on an affected device. The vulnerability exists because the affected software incorrectly runs the SFTP user service at the privilege level of the account that was running when the ConfD built-in Secure Shell (SSH) server for CLI was enabled. If the ConfD built-in SSH server was not enabled, the device is not affected by this vulnerability. An attacker with low-level privileges could exploit this vulnerability by authenticating to an affected device and issuing a series of commands at the SFTP interface. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confd-priv-esc-LsGtCRx4, https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-priv-esc-XXqRtTfT	A-CIS-CONF-180821/47

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
			elevate privileges to the level of the account under which ConfD is running, which is commonly root. Note: Any user who can authenticate to the built-in SSH server may exploit this vulnerability. By default, all ConfD users have this access if the server is enabled. Software updates that address this vulnerability have been released. **CVE ID : CVE-2021-1572**		
connected_mobile_experiences					
Weak Password Requirements	04-Aug-21	4	A vulnerability in the change password API of Cisco Connected Mobile Experiences (CMX) could allow an authenticated, remote attacker to alter their own password to a value that does not comply with the strong authentication requirements that are configured on an affected device. This vulnerability exists because a password policy check is incomplete at the time a password is changed at server side using the API. An attacker could exploit this vulnerability by sending a specially crafted API request to the affected device. A successful exploit could allow the attacker to change their own password to a value that does not comply with the configured strong	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmx-GkCvfd4	A-CIS-CONN-180821/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication requirements. **CVE ID : CVE-2021-1522**		
evolved_programmable_network_manager					
Exposure of Sensitive Information to an Unauthorized Actor	04-Aug-21	4	A vulnerability in the REST API of Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to access sensitive data on an affected system. This vulnerability exists because the application does not sufficiently protect sensitive data when responding to an API request. An attacker could exploit the vulnerability by sending a specific API request to the affected application. A successful exploit could allow the attacker to obtain sensitive information about the application. **CVE ID : CVE-2021-34707**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-info-disc-PjTZ5r6C	A-CIS-EVOL-180821/49
network_services_orchestrator					
Improper Privilege Management	04-Aug-21	6.9	A vulnerability in ConfD could allow an authenticated, local attacker to execute arbitrary commands at the level of the account under which ConfD is running, which is commonly root. To exploit this vulnerability, an attacker must have a valid account on an affected device. The vulnerability exists because the affected software incorrectly runs the SFTP user	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confd-priv-esc-LsGtCRx4, https://tools.cisco.com/security/center/content/Cis	A-CIS-NETW-180821/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service at the privilege level of the account that was running when the ConfD built-in Secure Shell (SSH) server for CLI was enabled. If the ConfD built-in SSH server was not enabled, the device is not affected by this vulnerability. An attacker with low-level privileges could exploit this vulnerability by authenticating to an affected device and issuing a series of commands at the SFTP interface. A successful exploit could allow the attacker to elevate privileges to the level of the account under which ConfD is running, which is commonly root. Note: Any user who can authenticate to the built-in SSH server may exploit this vulnerability. By default, all ConfD users have this access if the server is enabled. Software updates that address this vulnerability have been released. **CVE ID : CVE-2021-1572**	coSecurityAdvisory/cisco-sa-nso-priv-esc-XXqRtTfT	
packet_tracer					
Uncontrolled Search Path Element	04-Aug-21	6.9	A vulnerability in Cisco Packet Tracer for Windows could allow an authenticated, local attacker to perform a DLL injection attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-packettracer-dll-inj-	A-CIS-PACK-180821/51

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path on the system, which can cause a malicious DLL file to be loaded when the application starts. A successful exploit could allow an attacker with normal user privileges to execute arbitrary code on the affected system with the privileges of another user&rsquo;s account. **CVE ID : CVE-2021-1593**	Qv8Mk5Jx	
Citrix					
application_delivery_management					
N/A	05-Aug-21	4.3	A vulnerability has been discovered in Citrix ADC (formerly known as NetScaler ADC) and Citrix Gateway (formerly known as NetScaler Gateway), and Citrix SD-WAN WANOP Edition models 4000-WO, 4100-WO, 5000-WO, and 5100-WO. These vulnerabilities, if exploited, could lead to a phishing attack through a SAML authentication hijack to steal a valid user session. **CVE ID : CVE-2021-22920**	https://support.citrix.com/article/CTX319135	A-CIT-APPL-180821/52
gateway					
N/A	05-Aug-21	4.3	A vulnerability has been discovered in Citrix ADC	https://support.citrix.com	A-CIT-GATE-180821/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(formerly known as NetScaler ADC) and Citrix Gateway (formerly known as NetScaler Gateway), and Citrix SD-WAN WANOP Edition models 4000-WO, 4100-WO, 5000-WO, and 5100-WO. These vulnerabilities, if exploited, could lead to a phishing attack through a SAML authentication hijack to steal a valid user session. **CVE ID : CVE-2021-22920**	/article/CTX319135	
virtual_apps_and_desktops					
Improper Privilege Management	05-Aug-21	7.2	A vulnerability has been identified in Citrix Virtual Apps and Desktops that could, if exploited, allow a user of a Windows VDA that has either Citrix Profile Management or Citrix Profile Management WMI Plugin installed to escalate their privilege level on that Windows VDA to SYSTEM. **CVE ID : CVE-2021-22928**	https://support.citrix.com/article/CTX319750	A-CIT-VIRT-180821/54
xenapp					
Improper Privilege Management	05-Aug-21	7.2	A vulnerability has been identified in Citrix Virtual Apps and Desktops that could, if exploited, allow a user of a Windows VDA that has either Citrix Profile Management or Citrix Profile Management WMI Plugin installed to escalate their privilege level on that Windows VDA to	https://support.citrix.com/article/CTX319750	A-CIT-XENA-180821/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SYSTEM. **CVE ID : CVE-2021-22928**		
xendesktop					
Improper Privilege Management	05-Aug-21	7.2	A vulnerability has been identified in Citrix Virtual Apps and Desktops that could, if exploited, allow a user of a Windows VDA that has either Citrix Profile Management or Citrix Profile Management WMI Plugin installed to escalate their privilege level on that Windows VDA to SYSTEM. **CVE ID : CVE-2021-22928**	https://support.citrix.com/article/CTX319750	A-CIT-XEND-180821/56
cmsuno_project					
cmsuno					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	3.5	CMSuno 1.7 is vulnerable to an authenticated stored cross site scripting in modifying the filename parameter (tgo) while updating the theme. **CVE ID : CVE-2021-36654**	N/A	A-CMS-CMSU-180821/57
Codesys					
development_system					
Deserialization of Untrusted Data	05-Aug-21	6.8	A unsafe deserialization vulnerability exists in the ComponentModel Profile.FromFile() functionality of CODESYS GmbH CODESYS Development System 3.5.16 and 3.5.17. A specially crafted file can lead to arbitrary command	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16805&token=ee583c498941d9fda86490bca98ff2	A-COD-DEVE-180821/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21863**	1928eec08a&download=	
Deserialization of Untrusted Data	02-Aug-21	6.8	A unsafe deserialization vulnerability exists in the ComponentModel ComponentManager.StartupCultureSettings functionality of CODESYS GmbH CODESYS Development System 3.5.16 and 3.5.17. A specially crafted file can lead to arbitrary command execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21864**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16805&token=ee583c498941d9fda86490bca98ff21928eec08a&download=	A-COD-DEVE-180821/59
Deserialization of Untrusted Data	02-Aug-21	6.8	A unsafe deserialization vulnerability exists in the PackageManagement.plugin ExtensionMethods.Clone() functionality of CODESYS GmbH CODESYS Development System 3.5.16. A specially crafted file can lead to arbitrary command execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21865**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16805&token=ee583c498941d9fda86490bca98ff21928eec08a&download=	A-COD-DEVE-180821/60
Deserialization of Untrusted Data	02-Aug-21	6.8	A unsafe deserialization vulnerability exists in the ObjectManager.plugin ProfileInformation.ProfileData functionality of CODESYS GmbH CODESYS Development System 3.5.16 and 3.5.17. A	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16805&token=ee583c49	A-COD-DEVE-180821/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted file can lead to arbitrary command execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2021-21866**	8941d9fda86490bca98ff21928eec08a&download=	
ethernetip					
NULL Pointer Dereference	04-Aug-21	5	In CODESYS EtherNetIP before 4.1.0.0, specific EtherNet/IP requests may cause a null pointer dereference in the downloaded vulnerable EtherNet/IP stack that is executed by the CODESYS Control runtime system. **CVE ID : CVE-2021-36765**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16806&token=3b0c51de5a6e35bccbb413ddaaa56551ca5490f6&download=	A-COD-ETHE-180821/62
gateway					
NULL Pointer Dereference	04-Aug-21	5	In CODESYS Gateway V3 before 3.5.17.10, there is a NULL Pointer Dereference. Crafted communication requests may cause a Null pointer dereference in the affected CODESYS products and may result in a denial-of-service condition. **CVE ID : CVE-2021-36764**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16804&token=d8c89c887979b22fdfc9fd5c3aa3804bbb1ddbff&download=	A-COD-GATE-180821/63
community_events_project					
community_events					
Improper Neutralization of Input During Web Page	02-Aug-21	4.3	The Community Events WordPress plugin before 1.4.8 does not sanitise, validate or escape its importrowscount and successimportcount GET	N/A	A-COM-COMM-180821/64

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			parameters before outputting them back in an admin page, leading to a reflected Cross-Site Scripting issue which will be executed in the context of a logged in administrator **CVE ID : CVE-2021-24496**		
comrak_project					
comrak					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-21	4.3	An issue was discovered in the comrak crate before 0.10.1 for Rust. It mishandles & characters, leading to XSS via &# HTML entities. **CVE ID : CVE-2021-38186**	https://rustsec.org/advisories/RUSTSEC-2021-0063.html	A-COM-COMR-180821/65
corero					
securewatch_managed_services					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Aug-21	4	Corero SecureWatch Managed Services 9.7.2.0020 is affected by a Path Traversal vulnerability via the snap_file parameter in the /it-IT/splunkd/__raw/services/get_snapshot HTTP API endpoint. A 'low privileged' attacker can read any file on the target host. **CVE ID : CVE-2021-38136**	N/A	A-COR-SECU-180821/66
Improper Authentication	06-Aug-21	5.5	Corero SecureWatch Managed Services 9.7.2.0020 does not correctly check swa-monitor and cns-monitor user's privileges, allowing a user to perform actions not belonging	N/A	A-COR-SECU-180821/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to his role. **CVE ID : CVE-2021-38137**		
Courier-mta					
mail_server					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Aug-21	6.8	An issue was discovered in the POP3 component of Courier Mail Server before 1.1.5. Meddler-in-the-middle attackers can pipeline commands after the POP3 STLS command, injecting plaintext commands into an encrypted user session. **CVE ID : CVE-2021-38084**	N/A	A-COU-MAIL-180821/68
cozmoslabs					
profile_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The User Registration & User Profile â€“ Profile Builder WordPress plugin before 3.4.8 does not sanitise or escape its 'Modify default Redirect Delay timer' setting, allowing high privilege users to use JavaScript code in it, even when the unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24448**	N/A	A-COZ-PROF-180821/69
user_profile_picture					
Authorization Bypass Through User-Controlled	02-Aug-21	5.5	The User Profile Picture WordPress plugin before 2.6.0 was affected by an IDOR issue, allowing users with the upload_image capability (by	N/A	A-COZ-USER-180821/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Key			default author and above) to change and delete the profile pictures of other users (including those with higher roles). **CVE ID : CVE-2021-24473**		
crossbeam_project					
crossbeam					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Aug-21	6.8	crossbeam-deque is a package of work-stealing deques for building task schedulers when programming in Rust. In versions prior to 0.7.4 and 0.8.0, the result of the race condition is that one or more tasks in the worker queue can be popped twice instead of other tasks that are forgotten and never popped. If tasks are allocated on the heap, this can cause double free and a memory leak. If not, this still can cause a logical bug. Crates using `Stealer::steal`, `Stealer::steal_batch`, or `Stealer::steal_batch_and_pop` are affected by this issue. This has been fixed in crossbeam-deque 0.8.1 and 0.7.4. **CVE ID : CVE-2021-32810**	https://github.com/crossbeam-rs/crossbeam/security/advisories/GHSA-pqqp-xmhj-wgcw	A-CRO-CROS-180821/71
ctparental_project					
ctparental					
Improper Neutralization of Input During Web Page	10-Aug-21	4.3	CTparental before 4.45.03 is vulnerable to cross-site scripting (XSS) in the CTparental admin panel. In bl_categires_help.php, the	N/A	A-CTP-CTPA-180821/72

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			'categories' variable is assigned with the content of the query string param 'cat' without sanitization or encoding, enabling an attacker to inject malicious code into the output webpage. **CVE ID : CVE-2021-37365**		
Cross-Site Request Forgery (CSRF)	10-Aug-21	6.8	CTparental before 4.45.03 is vulnerable to cross-site request forgery (CSRF) in the CTparental admin panel. By combining CSRF with XSS, an attacker can trick the administrator into clicking a link that cancels the filtering for all standard users. **CVE ID : CVE-2021-37366**	N/A	A-CTP-CTPA-180821/73
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Aug-21	4.6	CTparental before 4.45.07 is affected by a code execution vulnerability in the CTparental admin panel. Because The file "bl_categories_help.php" is vulnerable to directory traversal, an attacker can create a file that contains scripts and run arbitrary commands. **CVE ID : CVE-2021-37367**	N/A	A-CTP-CTPA-180821/74
Dell					
openmanage_enterprise					
Improper Authentication	09-Aug-21	7.5	Dell OpenManage Enterprise versions prior to 3.6.1 contain an improper authentication vulnerability. A remote unauthenticated attacker may	https://www.dell.com/support/kbdoc/000189673	A-DEL-OPEN-180821/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit this vulnerability to hijack an elevated session or perform unauthorized actions by sending malformed data. **CVE ID : CVE-2021-21564**		
Exposure of Sensitive Information to an Unauthorized Actor	09-Aug-21	4	Dell OpenManage Enterprise version 3.5 and OpenManage Enterprise-Modular version 1.30.00 contain an information disclosure vulnerability. An authenticated low privileged attacker may potentially exploit this vulnerability leading to disclosure of the OIDC server credentials. **CVE ID : CVE-2021-21584**	https://www.dell.com/support/kbdoc/000189673	A-DEL-OPEN-180821/76
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Aug-21	9	Dell OpenManage Enterprise versions prior to 3.6.1 contain an OS command injection vulnerability in RACADM and IPMI tools. A remote authenticated malicious user with high privileges may potentially exploit this vulnerability to execute arbitrary OS commands. **CVE ID : CVE-2021-21585**	https://www.dell.com/support/kbdoc/000189673	A-DEL-OPEN-180821/77
Exposure of Sensitive Information to an Unauthorized Actor	09-Aug-21	5.8	Dell OpenManage Enterprise versions 3.4 through 3.6.1 and Dell OpenManage Enterprise Modular versions 1.20.00 through 1.30.00, contain a remote code execution vulnerability. A malicious attacker with access to the immediate subnet may	https://www.dell.com/support/kbdoc/000189673	A-DEL-OPEN-180821/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit this vulnerability leading to information disclosure and a possible elevation of privileges. **CVE ID : CVE-2021-21596**		
openmanage_enterprise-modular					
Exposure of Sensitive Information to an Unauthorized Actor	09-Aug-21	4	Dell OpenManage Enterprise version 3.5 and OpenManage Enterprise-Modular version 1.30.00 contain an information disclosure vulnerability. An authenticated low privileged attacker may potentially exploit this vulnerability leading to disclosure of the OIDC server credentials. **CVE ID : CVE-2021-21584**	https://www.dell.com/support/kbdoc/000189673	A-DEL-OPEN-180821/79
Exposure of Sensitive Information to an Unauthorized Actor	09-Aug-21	5.8	Dell OpenManage Enterprise versions 3.4 through 3.6.1 and Dell OpenManage Enterprise Modular versions 1.20.00 through 1.30.00, contain a remote code execution vulnerability. A malicious attacker with access to the immediate subnet may potentially exploit this vulnerability leading to information disclosure and a possible elevation of privileges. **CVE ID : CVE-2021-21596**	https://www.dell.com/support/kbdoc/000189673	A-DEL-OPEN-180821/80
powerscale_onefs					
N/A	03-Aug-21	7.2	Dell PowerScale OneFS versions 8.1.0-9.1.0 contain	https://www.dell.com/sup	A-DEL-POWE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an Incorrect User Management vulnerability.under some specific conditions, this can allow the CompAdmin user to elevate privileges and break out of Compliance mode. This is a critical vulnerability and Dell recommends upgrading at the earliest. **CVE ID : CVE-2021-21553**	port/kbdoc/ 000188148	180821/81
Uncontrolled Resource Consumption	03-Aug-21	5	Dell PowerScale OneFS versions 9.1.0.3 and earlier contain a denial of service vulnerability. SmartConnect had an error condition that may be triggered to loop, using CPU and potentially preventing other SmartConnect DNS responses. **CVE ID : CVE-2021-21565**	https://www .dell.com/sup port/kbdoc/ 000188148	A-DEL-POWE-180821/82
Devexpress					
devexpress					
Deserialization of Untrusted Data	04-Aug-21	7.5	DevExpress.XtraReports.UI through v21.1 allows attackers to execute arbitrary code via insecure deserialization. **CVE ID : CVE-2021-36483**	N/A	A-DEV-DEVE-180821/83
digitaldruid					
hoteldruid					
Improper Neutralization of Special Elements used in an	03-Aug-21	7.5	A SQL injection vulnerability exists in version 3.0.2 of Hotel Druid when SQLite is being used as the application database. A malicious attacker	N/A	A-DIG-HOTE-180821/84

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			can issue SQL commands to the SQLite database through the vulnerable idappartamenti parameter. **CVE ID : CVE-2021-37832**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	4.3	A reflected cross-site scripting (XSS) vulnerability exists in multiple pages in version 3.0.2 of the Hotel Druid application that allows for arbitrary execution of JavaScript commands. **CVE ID : CVE-2021-37833**	N/A	A-DIG-HOTE-180821/85
doft					
doftcoin					
Integer Overflow or Wraparound	03-Aug-21	5	An integer overflow in the mintToken function of a smart contract implementation for Doftcoin Token, an Ethereum ERC20 token, allows the owner to cause unexpected financial losses. **CVE ID : CVE-2021-34270**	N/A	A-DOF-DOFT-180821/86
drawblog_project					
drawblog					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The DrawBlog WordPress plugin through 0.90 does not sanitise or validate some of its settings before outputting them back in the page, leading to an authenticated stored Cross-Site Scripting issue **CVE ID : CVE-2021-24479**	N/A	A-DRA-DRAW-180821/87
dreamsecurity					
magicline4nx.exe					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Aug-21	10	A vulnerability in PKI Security Solution of Dream Security could allow arbitrary command execution. This vulnerability is due to insufficient validation of the authorization certificate. An attacker could exploit this vulnerability by sending a crafted HTTP request an affected program. A successful exploit could allow the attacker to remotely execute arbitrary code on a target system. **CVE ID : CVE-2021-26606**	N/A	A-DRE-MAGI-180821/88
drogon					
drogon					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-21	5	A path traversal vulnerability in the static router for Drogon from 1.0.0-beta14 to 1.6.0 could allow an unauthenticated, remote attacker to arbitrarily read files. The vulnerability is due to lack of proper input validation for requested path. An attacker could exploit this vulnerability by sending crafted HTTP request with specific path to read. Successful exploitation could allow the attacker to read files that should be restricted. **CVE ID : CVE-2021-35397**	N/A	A-DRO-DROG-180821/89
dwbooster					
calendar_event_multi_view					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	4.3	The Calendar Event Multi View WordPress plugin before 1.4.01 does not sanitise or escape the 'start' and 'end' GET parameters before outputting them in the page (via php/edit.php), leading to a reflected Cross-Site Scripting issue. **CVE ID : CVE-2021-24498**	N/A	A-DWB-CALE-180821/90
electronjs					
poddycast					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Aug-21	4.3	Poddycast is a podcast app made with Electron. Prior to version 0.8.1, an attacker can create a podcast or episode with malicious characters and execute commands on the client machine. The application does not clean the HTML characters of the podcast information obtained from the Feed, which allows the injection of HTML and JS code (cross-site scripting). Being an application made in electron, cross-site scripting can be scaled to remote code execution, making it possible to execute commands on the machine where the application is running. The vulnerability is patched in Poddycast version 0.8.1. **CVE ID : CVE-2021-32772**	https://github.com/MrChuckomo/poddycast/security/advisories/GHSA-wjmh-9fj2-rqh6	A-ELE-PODD-180821/91
entando					
admin_console					

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 in Output Used by a Downstream Component ('Injection')	02-Aug-21	9	A Server Side Template Injection in the Entando Admin Console 6.3.9 and before allows a user with privileges to execute FreeMarker template with command execution via freemarker.template.utility.Execute **CVE ID : CVE-2021-35450**	N/A	A-ENT-ADMI-180821/92
Espocrm					
espocrm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	3.5	EspoCRM 6.1.6 and prior suffers from a persistent (type II) cross-site scripting (XSS) vulnerability in processing user-supplied avatar images. This issue was fixed in version 6.1.7 of the product. **CVE ID : CVE-2021-3539**	N/A	A-ESP-ESPO-180821/93
event_geek_project					
event_geek					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The Event Geek WordPress plugin through 2.5.2 does not sanitise or escape its "Use your own " setting before outputting it in the page, leading to an authenticated (admin+) stored Cross-Site Scripting issue **CVE ID : CVE-2021-24480**	N/A	A-EVE-EVEN-180821/94
F-secure					
business_suite					
N/A	05-Aug-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby	https://www.f-secure.com/e	A-F-S-BUSI-180821/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33597**	n/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories	
client_security					
N/A	05-Aug-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33597**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-CLIE-180821/96
elements_endpoint_protection					
N/A	05-Aug-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products	https://www.f-secure.com/en/business/programs/vul	A-F-S-ELEM-180821/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33597**	nerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories	
linux_security					
N/A	05-Aug-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33597**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-LINU-180821/98
safe					
Improper Restriction of Rendered UI Layers or Frames	05-Aug-21	3.5	Showing the legitimate URL in the address bar while loading the content from other domain. This makes the user believe that the content is served by a legit domain. Exploiting the vulnerability	https://www.f-secure.com/en/business/programs/vulnerability-reward-	A-F-S-SAFE-180821/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requires the user to click on a specially crafted, seemingly legitimate URL containing an embedded malicious redirect while using F-Secure Safe Browser for iOS. **CVE ID : CVE-2021-33596**	program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories	
Ffmpeg					
ffmpeg					
N/A	05-Aug-21	4.3	Prior to ffmpeg version 4.3, the tty demuxer did not have a 'read_probe' function assigned to it. By crafting a legitimate "ffconcat" file that references an image, followed by a file the triggers the tty demuxer, the contents of the second file will be copied into the output file verbatim (as long as the `-vcodec copy` option is passed to ffmpeg). **CVE ID : CVE-2021-3566**	https://github.com/FFmpeg/FFmpeg/commit/3bce9e9b3ea35c54bacccc793d7da99ea5157532#diff-74f6b92a0541378ad15de9c29c0a2b0c69881ad9ffc71abe568b88b535e00a7f	A-FFM-FFMP-180821/100
Unchecked Return Value	04-Aug-21	4.3	libavcodec/dnxhddec.c in FFmpeg 4.4 does not check the return value of the init_vlc function, a similar issue to CVE-2013-0868. **CVE ID : CVE-2021-38114**	https://github.com/FFmpeg/FFmpeg/commit/7150f9575671f898382c370acae35f9087a30ba1, https://patchwork.ffmpeg.org/project/ffmpeg/patch	A-FFM-FFMP-180821/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/PAXP193MB12624C21AE412BE95BA4D4A4B6F09@PAXP193MB1262.EURP193.PROD.OUTLOOK.COM/	
Fortinet					
fortianalyzer					
Incorrect Authorization	06-Aug-21	4	An improper access control vulnerability in FortiManager and FortiAnalyzer GUI interface 7.0.0, 6.4.5 and below, 6.2.8 and below, 6.0.11and below, 5.6.11and below may allow a remote and authenticated attacker with restricted user profile to retrieve the list of administrative users of other ADOMs and their related configuration. **CVE ID : CVE-2021-32587**	https://fortiguard.com/advisory/FG-IR-21-059	A-FOR-FORT-180821/102
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-21	3.5	Multiple improper neutralization of input during web page generation (CWE-79) in FortiManager and FortiAnalyzer versions 7.0.0, 6.4.5 and below, 6.2.7 and below user interface, may allow a remote authenticated attacker to perform a Stored Cross Site Scripting attack (XSS) by injecting malicious payload in GET parameters.	https://fortiguard.com/advisory/FG-IR-21-054	A-FOR-FORT-180821/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-32597		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	05-Aug-21	4	An improper neutralization of CRLF sequences in HTTP headers ('HTTP Response Splitting') vulnerability In FortiManager and FortiAnalyzer GUI 7.0.0, 6.4.6 and below, 6.2.8 and below, 6.0.11 and below, 5.6.11 and below may allow an authenticated and remote attacker to perform an HTTP request splitting attack which gives attackers control of the remaining headers and body of the response. **CVE ID : CVE-2021-32598**	https://fortiguard.com/advisory/FG-IR-21-063	A-FOR-FORT-180821/104
Server-Side Request Forgery (SSRF)	05-Aug-21	4	A server-side request forgery (SSRF) (CWE-918) vulnerability in FortiManager and FortiAnalyser GUI 7.0.0, 6.4.5 and below, 6.2.7 and below, 6.0.11 and below, 5.6.11 and below may allow a remote and authenticated attacker to access unauthorized files and services on the system via specifically crafted web requests. **CVE ID : CVE-2021-32603**	https://fortiguard.com/advisory/FG-IR-21-050	A-FOR-FORT-180821/105
fortiauthenticator					
Uncontrolled Resource Consumption	04-Aug-21	7.8	An uncontrolled resource consumption (denial of service) vulnerability in the login modules of FortiSandbox 3.2.0 through 3.2.2, 3.1.0 through 3.1.4, and	https://fortiguard.com/advisory/FG-IR-20-170	A-FOR-FORT-180821/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.0.0 through 3.0.6; and FortiAuthenticator before 6.0.6 may allow an unauthenticated attacker to bring the device into an unresponsive state via specifically-crafted long request parameters. **CVE ID : CVE-2021-22124**		
fortimanager					
Incorrect Authorization	06-Aug-21	4	An improper access control vulnerability in FortiManager and FortiAnalyzer GUI interface 7.0.0, 6.4.5 and below, 6.2.8 and below, 6.0.11and below, 5.6.11and below may allow a remote and authenticated attacker with restricted user profile to retrieve the list of administrative users of other ADOMs and their related configuration. **CVE ID : CVE-2021-32587**	https://fortiguard.com/advisory/FG-IR-21-059	A-FOR-FORT-180821/107
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-21	3.5	Multiple improper neutralization of input during web page generation (CWE-79) in FortiManager and FortiAnalyzer versions 7.0.0, 6.4.5 and below, 6.2.7 and below user interface, may allow a remote authenticated attacker to perform a Stored Cross Site Scripting attack (XSS) by injecting malicious payload in GET parameters. **CVE ID : CVE-2021-32597**	https://fortiguard.com/advisory/FG-IR-21-054	A-FOR-FORT-180821/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	05-Aug-21	4	An improper neutralization of CRLF sequences in HTTP headers ('HTTP Response Splitting') vulnerability In FortiManager and FortiAnalyzer GUI 7.0.0, 6.4.6 and below, 6.2.8 and below, 6.0.11 and below, 5.6.11 and below may allow an authenticated and remote attacker to perform an HTTP request splitting attack which gives attackers control of the remaining headers and body of the response. **CVE ID : CVE-2021-32598**	https://fortiguard.com/advisory/FG-IR-21-063	A-FOR-FORT-180821/109
Server-Side Request Forgery (SSRF)	05-Aug-21	4	A server-side request forgery (SSRF) (CWE-918) vulnerability in FortiManager and FortiAnalyser GUI 7.0.0, 6.4.5 and below, 6.2.7 and below, 6.0.11 and below, 5.6.11 and below may allow a remote and authenticated attacker to access unauthorized files and services on the system via specifically crafted web requests. **CVE ID : CVE-2021-32603**	https://fortiguard.com/advisory/FG-IR-21-050	A-FOR-FORT-180821/110
fortiportal					
Improper Neutralization of Special Elements used in an SQL Command	04-Aug-21	9	Multiple improper neutralization of special elements used in an SQL command vulnerabilities in FortiPortal 6.0.0 through 6.0.4, 5.3.0 through 5.3.5, 5.2.0 through 5.2.5, and 4.2.2	https://fortiguard.com/advisory/FG-IR-21-084	A-FOR-FORT-180821/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			and earlier may allow an attacker with regular user's privileges to execute arbitrary commands on the underlying SQL database via specifically crafted HTTP requests. **CVE ID : CVE-2021-32590**		
Unrestricted Upload of File with Dangerous Type	04-Aug-21	5.5	An unrestricted file upload vulnerability in the web interface of FortiPortal 6.0.0 through 6.0.4, 5.3.0 through 5.3.5, 5.2.0 through 5.2.5, and 4.2.2 and earlier may allow a low-privileged user to potentially tamper with the underlying system's files via the upload of specifically crafted files. **CVE ID : CVE-2021-32594**	https://fortiguard.com/advisory/FG-IR-21-092	A-FOR-FORT-180821/112
Use of Password Hash With Insufficient Computational Effort	04-Aug-21	5	A use of one-way hash with a predictable salt vulnerability in the password storing mechanism of FortiPortal 6.0.0 through 6.04 may allow an attacker already in possession of the password store to decrypt the passwords by means of precomputed tables. **CVE ID : CVE-2021-32596**	https://fortiguard.com/advisory/FG-IR-21-094	A-FOR-FORT-180821/113
Improper Limitation of a Pathname to a Restricted Directory ('Path	04-Aug-21	4	A Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') in Fortinet FortiPortal 6.x before 6.0.5, FortiPortal 5.3.x before 5.3.6 and any FortiPortal before 6.2.5 allows authenticated attacker to	https://fortiguard.com/advisory/FG-IR-21-085	A-FOR-FORT-180821/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			disclosure information via crafted GET request with malicious parameter values. **CVE ID : CVE-2021-36168**		
fortisandbox					
Uncontrolled Resource Consumption	04-Aug-21	7.8	An uncontrolled resource consumption (denial of service) vulnerability in the login modules of FortiSandbox 3.2.0 through 3.2.2, 3.1.0 through 3.1.4, and 3.0.0 through 3.0.6; and FortiAuthenticator before 6.0.6 may allow an unauthenticated attacker to bring the device into an unresponsive state via specifically-crafted long request parameters. **CVE ID : CVE-2021-22124**	https://fortiguard.com/advisory/FG-IR-20-170	A-FOR-FORT-180821/115
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-21	4	Improper limitation of a pathname to a restricted directory vulnerabilities in FortiSandbox 3.2.0 through 3.2.2, and 3.1.0 through 3.1.4 may allow an authenticated user to obtain unauthorized access to files and data via specifially crafted web requests. **CVE ID : CVE-2021-24010**	https://fortiguard.com/advisory/FG-IR-20-202	A-FOR-FORT-180821/116
Improper Neutralization of Input During Web Page Generation	04-Aug-21	4.3	Multiple instances of improper neutralization of input during web page generation vulnerabilities in FortiSandbox before 4.0.0 may allow an unauthenticated	https://fortiguard.com/advisory/FG-IR-20-209	A-FOR-FORT-180821/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to perform an XSS attack via specifically crafted request parameters. **CVE ID : CVE-2021-24014**		
Out-of-bounds Write	04-Aug-21	6.5	Multiple instances of heap-based buffer overflow in the command shell of FortiSandbox before 4.0.0 may allow an authenticated attacker to manipulate memory and alter its content by means of specifically crafted command line arguments. **CVE ID : CVE-2021-26096**	https://fortiguard.com/advisory/FG-IR-20-188	A-FOR-FORT-180821/118
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Aug-21	6.5	An improper neutralization of special elements used in an OS Command vulnerability in FortiSandbox 3.2.0 through 3.2.2, 3.1.0 through 3.1.4, and 3.0.0 through 3.0.6 may allow an authenticated attacker with access to the web GUI to execute unauthorized code or commands via specifically crafted HTTP requests. **CVE ID : CVE-2021-26097**	https://fortiguard.com/advisory/FG-IR-20-198	A-FOR-FORT-180821/119
Use of Insufficiently Random Values	04-Aug-21	5	An instance of small space of random values in the RPC API of FortiSandbox before 4.0.0 may allow an attacker in possession of a few information pieces about the state of the device to possibly predict valid session IDs. **CVE ID : CVE-2021-26098**	https://fortiguard.com/advisory/FG-IR-20-218	A-FOR-FORT-180821/120
Foxitsoftware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
foxit_reader					
Out-of-bounds Write	11-Aug-21	7.5	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write because the Cross-Reference table is mishandled during Office document conversion. **CVE ID : CVE-2021-33793**	https://www.foxitsoftware.com/support/security-bulletins.html	A-FOX-FOXI-180821/121
N/A	11-Aug-21	6.4	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 allow information disclosure or an application crash after mishandling the Tab key during XFA form interaction. **CVE ID : CVE-2021-33794**	https://www.foxitsoftware.com/support/security-bulletins.html	A-FOX-FOXI-180821/122
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Aug-21	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows memory corruption during conversion of a PDF document to a different document format. **CVE ID : CVE-2021-38568**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-180821/123
Uncontrolled Recursion	11-Aug-21	5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows stack consumption via recursive function calls during the handling of XFA forms or link objects. **CVE ID : CVE-2021-38569**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-180821/124
Improper Link Resolution Before File	11-Aug-21	6.4	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows attackers to delete	https://www.foxitsoftware.com/support/security-	A-FOX-FOXI-180821/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			arbitrary files (during uninstallation) via a symlink. **CVE ID : CVE-2021-38570**	bulletins.php	
Uncontrolled Search Path Element	11-Aug-21	4.4	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows DLL hijacking, aka CNVD-C-2021-68000 and CNVD-C-2021-68502. **CVE ID : CVE-2021-38571**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-180821/126
N/A	11-Aug-21	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows writing to arbitrary files because the extractPages pathname is not validated. **CVE ID : CVE-2021-38572**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-180821/127
N/A	11-Aug-21	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows writing to arbitrary files because a CombineFiles pathname is not validated. **CVE ID : CVE-2021-38573**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-180821/128
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Aug-21	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows SQL Injection via crafted data at the end of a string. **CVE ID : CVE-2021-38574**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-180821/129
pdf_editor					
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute	https://www.foxit.com/su	A-FOX-PDF_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on affected installations of Foxit Reader 10.1.4.37651. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Document objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13741. **CVE ID : CVE-2021-34831**	pport/security-bulletins.html	180821/130
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the delay property. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CAN-13928. **CVE ID : CVE-2021-34832**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14023. **CVE ID : CVE-2021-34833**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/132
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14014. **CVE ID : CVE-2021-34834**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14015. **CVE ID : CVE-2021-34835**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/134
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/135

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
			malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14017. **CVE ID : CVE-2021-34836**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14018. **CVE ID : CVE-2021-34837**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/136
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute	https://www.foxit.com/su	A-FOX-PDF_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14019. **CVE ID : CVE-2021-34838**	pport/security-bulletins.html	180821/137
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the current process. Was ZDI-CAN-14020. **CVE ID : CVE-2021-34839**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14021. **CVE ID : CVE-2021-34840**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/139
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14022. **CVE ID : CVE-2021-34841**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14024. **CVE ID : CVE-2021-34842**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/141
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14025. **CVE ID : CVE-2021-34843**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14033. **CVE ID : CVE-2021-34844**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/143
Use After	04-Aug-21	6.8	This vulnerability allows	https://www	A-FOX-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14034. **CVE ID : CVE-2021-34845**	.foxit.com/support/security-bulletins.html	PDF_-180821/144
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the current process. Was ZDI-CAN-14120. **CVE ID : CVE-2021-34846**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14270. **CVE ID : CVE-2021-34847**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/146
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14532. **CVE ID : CVE-2021-34848**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14531. **CVE ID : CVE-2021-34849**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/148
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14529. **CVE ID : CVE-2021-34850**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14016. **CVE ID : CVE-2021-34851**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13929. **CVE ID : CVE-2021-34852**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/151
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14013. **CVE ID : CVE-2021-34853**		
pdf_reader					
Use After Free	05-Aug-21	6.8	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 10.1.3.37598. A specially crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled. **CVE ID : CVE-2021-21831**	N/A	A-FOX-PDF_-180821/153
Use After Free	05-Aug-21	6.8	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 10.1.4.37651. A specially crafted PDF document can trigger the reuse of previously free memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening a malicious file or site to trigger this vulnerability if the browser plugin extension is enabled.	N/A	A-FOX-PDF_-180821/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21870		
Use After Free	05-Aug-21	6.8	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 11.0.0.49893. A specially crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled. **CVE ID : CVE-2021-21893**	N/A	A-FOX-PDF_-180821/155
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.4.37651. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Document objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CAN-13741. **CVE ID : CVE-2021-34831**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the delay property. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13928. **CVE ID : CVE-2021-34832**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/157
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14023. **CVE ID : CVE-2021-34833**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14014. **CVE ID : CVE-2021-34834**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/159
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14015. **CVE ID : CVE-2021-34835**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14017. **CVE ID : CVE-2021-34836**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/161
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute	https://www.foxit.com/su	A-FOX-PDF_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14018. **CVE ID : CVE-2021-34837**	pport/security-bulletins.html	180821/162
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the current process. Was ZDI-CAN-14019. **CVE ID : CVE-2021-34838**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14020. **CVE ID : CVE-2021-34839**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/164
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14021. **CVE ID : CVE-2021-34840**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14022. **CVE ID : CVE-2021-34841**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/166
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14024. **CVE ID : CVE-2021-34842**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14025. **CVE ID : CVE-2021-34843**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/168
Use After	04-Aug-21	6.8	This vulnerability allows	https://www	A-FOX-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14033. **CVE ID : CVE-2021-34844**	.foxit.com/support/security-bulletins.html	PDF_-180821/169
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the current process. Was ZDI-CAN-14034. **CVE ID : CVE-2021-34845**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14120. **CVE ID : CVE-2021-34846**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/171
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14270. **CVE ID : CVE-2021-34847**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14532. **CVE ID : CVE-2021-34848**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/173
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14531. **CVE ID : CVE-2021-34849**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14529. **CVE ID : CVE-2021-34850**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14016. **CVE ID : CVE-2021-34851**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/176
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13929. **CVE ID : CVE-2021-34852**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14013. **CVE ID : CVE-2021-34853**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-180821/178
phantompdf					
Out-of-bounds Write	11-Aug-21	7.5	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write because the Cross-Reference table is mishandled during Office document conversion. **CVE ID : CVE-2021-33793**	https://www.foxitsoftware.com/support/security-bulletins.html	A-FOX-PHAN-180821/179
N/A	11-Aug-21	6.4	Foxit Reader before 10.1.4	https://www	A-FOX-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and PhantomPDF before 10.1.4 allow information disclosure or an application crash after mishandling the Tab key during XFA form interaction. **CVE ID : CVE-2021-33794**	.foxitsoftware.com/support/security-bulletins.html	PHAN-180821/180
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-Aug-21	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows memory corruption during conversion of a PDF document to a different document format. **CVE ID : CVE-2021-38568**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-180821/181
Uncontrolled Recursion	11-Aug-21	5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows stack consumption via recursive function calls during the handling of XFA forms or link objects. **CVE ID : CVE-2021-38569**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-180821/182
Improper Link Resolution Before File Access ('Link Following')	11-Aug-21	6.4	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows attackers to delete arbitrary files (during uninstallation) via a symlink. **CVE ID : CVE-2021-38570**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-180821/183
Uncontrolled Search Path Element	11-Aug-21	4.4	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows DLL hijacking, aka CNVD-C-2021-68000 and CNVD-C-2021-68502.	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-180821/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-38571		
N/A	11-Aug-21	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows writing to arbitrary files because the extractPages pathname is not validated. **CVE ID : CVE-2021-38572**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-180821/185
N/A	11-Aug-21	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows writing to arbitrary files because a CombineFiles pathname is not validated. **CVE ID : CVE-2021-38573**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-180821/186
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Aug-21	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows SQL Injection via crafted data at the end of a string. **CVE ID : CVE-2021-38574**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-180821/187
Freebsd					
libfetch					
Out-of-bounds Read	03-Aug-21	6.4	libfetch before 2021-07-26, as used in apk-tools, xbps, and other products, mishandles numeric strings for the FTP and HTTP protocols. The FTP passive mode implementation allows an out-of-bounds read because strtol is used to parse the relevant numbers into address bytes. It does not check if the line ends	https://github.com/freebsd/freebsd-src/commits/main/lib/libfetch	A-FRE-LIBF-180821/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prematurely. If it does, the for-loop condition checks for the '\0' terminator one byte too late. **CVE ID : CVE-2021-36159**		
gestionaleamica					
amica_prodigy					
Incorrect Default Permissions	06-Aug-21	7.2	A vulnerability was found in CIR 2000 / Gestionale Amica Prodigy v1.7. The Amica Prodigy's executable "RemoteBackup.Service.exe" has incorrect permissions, allowing a local unprivileged user to replace it with a malicious file that will be executed with "LocalSystem" privileges. **CVE ID : CVE-2021-35312**	N/A	A-GES-AMIC-180821/189
Gitlab					
gitlab					
N/A	05-Aug-21	4	An issue has been discovered in GitLab CE/EE affecting all versions starting with 13.11, 13.12 and 14.0. A specially crafted design image allowed attackers to read arbitrary files on the server. **CVE ID : CVE-2021-22234**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22234.json	A-GIT-GITL-180821/190
Incorrect Authorization	05-Aug-21	4	Improper access control in GitLab EE versions 13.11.6, 13.12.6, and 14.0.2 allows users to be created via single sign on despite user cap being enabled **CVE ID : CVE-2021-22240**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22240.json	A-GIT-GITL-180821/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-21	3.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.0. It was possible to exploit a stored cross-site-scripting via a specifically crafted default branch name. **CVE ID : CVE-2021-22241**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22241.json	A-GIT-GITL-180821/192
Golang					
go					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-Aug-21	7.5	Go before 1.15.13 and 1.16.x before 1.16.5 has functions for DNS lookups that do not validate replies from DNS servers, and thus a return value may contain an unsafe injection (e.g., XSS) that does not conform to the RFC1035 format. **CVE ID : CVE-2021-33195**	https://groups.google.com/g/golang-announce/c/RgCMkAEQjSI	A-GOL-GO-180821/193
Uncontrolled Resource Consumption	02-Aug-21	5	In archive/zip in Go before 1.15.13 and 1.16.x before 1.16.5, a crafted file count (in an archive's header) can cause a NewReader or OpenReader panic. **CVE ID : CVE-2021-33196**	https://groups.google.com/g/golang-announce/c/RgCMkAEQjSI	A-GOL-GO-180821/194
Missing Authorization	02-Aug-21	4.3	In Go before 1.15.13 and 1.16.x before 1.16.5, some configurations of ReverseProxy (from net/http/httputil) result in a situation where an attacker is able to drop arbitrary headers. **CVE ID : CVE-2021-33197**	https://groups.google.com/g/golang-announce/c/RgCMkAEQjSI	A-GOL-GO-180821/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Aug-21	5	In Go before 1.15.13 and 1.16.x before 1.16.5, there can be a panic for a large exponent to the math/big.Rat SetString or UnmarshalText method. **CVE ID : CVE-2021-33198**	https://groups.google.com/g/golang-announce/c/RgCMkAEQjSI	A-GOL-GO-180821/196
Google					
asylo					
Out-of-bounds Read	02-Aug-21	2.1	An untrusted memory read vulnerability in Asylo versions up to 0.6.1 allows an untrusted attacker to pass a syscall number in MessageReader that is then used by sysno() and can bypass validation. This can allow the attacker to read memory from within the secure enclave. We recommend updating to Asylo 0.6.3 or past https://github.com/google/asylo/commit/90d7619e9dd99bcdb6cd28c7649d741d254d9a1a **CVE ID : CVE-2021-22552**	https://github.com/google/asylo/commit/90d7619e9dd99bcdb6cd28c7649d741d254d9a1a	A-GOO-ASYL-180821/197
chrome					
Use After Free	03-Aug-21	6.8	Use after free in V8 in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30541**	https://crbug.com/1214842, https://chromereleases.googleblog.com/2021/07/stable-channel-	A-GOO-CHRO-180821/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				update-for-desktop.html	
Out-of-bounds Write	03-Aug-21	6.8	Out of bounds write in ANGLE in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30559**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html, https://crbug.com/1219082	A-GOO-CHRO-180821/199
Use After Free	03-Aug-21	6.8	Use after free in Blink XSLT in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30560**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html, https://crbug.com/1219209	A-GOO-CHRO-180821/200
Access of Resource Using Incompatible Type ('Type Confusion')	03-Aug-21	6.8	Type Confusion in V8 in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30561**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html, https://crbug.com/1219630	A-GOO-CHRO-180821/201
Use After Free	03-Aug-21	6.8	Use after free in WebSerial in Google Chrome prior to 91.0.4472.164 allowed a	https://chromereleases.googleblog.co	A-GOO-CHRO-180821/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30562**	m/2021/07/stable-channel-update-for-desktop.html, https://crbug.com/1220078	
Access of Resource Using Incompatible Type ('Type Confusion')	03-Aug-21	6.8	Type Confusion in V8 in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30563**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html, https://crbug.com/1228407	A-GOO-CHRO-180821/203
Out-of-bounds Write	03-Aug-21	6.8	Heap buffer overflow in WebXR in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30564**	https://crbug.com/1221309, https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html	A-GOO-CHRO-180821/204
Out-of-bounds Write	03-Aug-21	6.8	Out of bounds write in Tab Groups in Google Chrome on Linux and ChromeOS prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a	https://crbug.com/1210985, https://chromereleases.googleblog.com/2021/07/stable-channel-	A-GOO-CHRO-180821/205

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
			crafted HTML page. **CVE ID : CVE-2021-30565**	update-for-desktop_20.html	
Out-of-bounds Write	03-Aug-21	6.8	Stack buffer overflow in Printing in Google Chrome prior to 92.0.4515.107 allowed a remote attacker who had compromised the renderer process to potentially exploit stack corruption via a crafted HTML page. **CVE ID : CVE-2021-30566**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html, https://crbug.com/1202661	A-GOO-CHRO-180821/206
Use After Free	03-Aug-21	6.8	Use after free in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to open DevTools to potentially exploit heap corruption via specific user gesture. **CVE ID : CVE-2021-30567**	https://crbug.com/1211326, https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/207
Out-of-bounds Write	03-Aug-21	6.8	Heap buffer overflow in WebGL in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30568**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/208
Use After Free	03-Aug-21	6.8	Use after free in sqlite in Google Chrome prior to	https://chromereleases.g	A-GOO-CHRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30569**	oogleblog.com/2021/07/stable-channel-update-for-desktop_20.html	180821/209
Incorrect Authorization	03-Aug-21	6.8	Insufficient policy enforcement in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2021-30571**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/210
Use After Free	03-Aug-21	6.8	Use after free in Autofill in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30572**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/211
Use After Free	03-Aug-21	6.8	Use after free in GPU in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30573**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/212
Use After Free	03-Aug-21	6.8	Use after free in protocol handling in Google Chrome prior to 92.0.4515.107	https://chromereleases.googleblog.co	A-GOO-CHRO-180821/213

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
			allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30574**	m/2021/07/stable-channel-update-for-desktop_20.html	
Out-of-bounds Write	03-Aug-21	6.8	Out of bounds write in Autofill in Google Chrome prior to 92.0.4515.107 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30575**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/214
Use After Free	03-Aug-21	6.8	Use after free in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30576**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/215
Incorrect Authorization	03-Aug-21	6.8	Insufficient policy enforcement in Installer in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to perform local privilege escalation via a crafted file. **CVE ID : CVE-2021-30577**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/216
Use of Uninitialized Resource	03-Aug-21	6.8	Uninitialized use in Media in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to perform out of bounds memory access	https://chromereleases.googleblog.com/2021/07/stable-	A-GOO-CHRO-180821/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. **CVE ID : CVE-2021-30578**	channel-update-for-desktop_20.html	
Use After Free	03-Aug-21	6.8	Use after free in UI framework in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30579**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/218
Incorrect Authorization	03-Aug-21	4.3	Insufficient policy enforcement in Android intents in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious application to obtain potentially sensitive information via a crafted HTML page. **CVE ID : CVE-2021-30580**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/219
Use After Free	03-Aug-21	6.8	Use after free in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30581**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/220
N/A	03-Aug-21	4.3	Inappropriate implementation in Animation in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to leak cross-	https://chromereleases.googleblog.com/2021/07/stable-	A-GOO-CHRO-180821/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			origin data via a crafted HTML page. **CVE ID : CVE-2021-30582**	channel-update-for-desktop_20.html	
Incorrect Authorization	03-Aug-21	4.3	Insufficient policy enforcement in image handling in iOS in Google Chrome on iOS prior to 92.0.4515.107 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-30583**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/222
N/A	03-Aug-21	4.3	Incorrect security UI in Downloads in Google Chrome on Android prior to 92.0.4515.107 allowed a remote attacker to perform domain spoofing via a crafted HTML page. **CVE ID : CVE-2021-30584**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/223
Use After Free	03-Aug-21	6.8	Use after free in sensor handling in Google Chrome on Windows prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30585**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/224
Use After Free	03-Aug-21	6.8	Use after free in dialog box handling in Windows in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to potentially	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-	A-GOO-CHRO-180821/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30586**	desktop_20.html	
N/A	03-Aug-21	4.3	Inappropriate implementation in Compositing in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2021-30587**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/226
Access of Resource Using Incompatible Type ('Type Confusion')	03-Aug-21	6.8	Type confusion in V8 in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2021-30588**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/227
Improper Input Validation	03-Aug-21	4.3	Insufficient validation of untrusted input in Sharing in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to bypass navigation restrictions via a crafted click-to-call link. **CVE ID : CVE-2021-30589**	https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-180821/228
gpac					
gpac					
Out-of-bounds Write	05-Aug-21	4.3	An issue was discovered in GPAC 1.0.1. There is a heap-based buffer overflow in the function	N/A	A-GPA-GPAC-180821/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			gp_rtp_builder_do_tx3g function in ietf/rtp_pck_3gpp.c, as demonstrated by MP4Box. This can cause a denial of service (DOS). **CVE ID : CVE-2021-36584**		
grafana					
loki					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-21	5	An issue was discovered in Grafana Loki through 2.2.1. The header value X-Scope-OrgID is used to construct file paths for rules files, and if crafted to conduct directory traversal such as ae ../../sensitive/path/in/deployment pathname, then Loki will attempt to parse a rules file at that location and include some of the contents in the error message. **CVE ID : CVE-2021-36156**	N/A	A-GRA-LOKI-180821/230
handsome_testimonials_\&_reviews_project					
handsome_testimonials_\&_reviews					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-21	6.5	The hndtst_action_instance_callback AJAX call of the Handsome Testimonials & Reviews WordPress plugin before 2.1.1, available to any authenticated users, does not sanitise, validate or escape the hndtst_previewShortcodeInstanceId POST parameter before using it in a SQL	https://codevigilant.com/disclosure/2021/wp-plugin-handsome-testimonials/	A-HAN-HAND-180821/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			statement, leading to an SQL Injection issue. **CVE ID : CVE-2021-24492**		
Haxx					
curl					
Insufficiently Protected Credentials	05-Aug-21	2.6	When curl is instructed to get content using the metalink feature, and a user name and password are used to download the metalink XML file, those same credentials are then subsequently passed on to each of the servers from which curl will download or try to download the contents from. Often contrary to the user's expectations and intentions and without telling the user it happened. **CVE ID : CVE-2021-22923**	N/A	A-HAX-CURL-180821/232
HP					
edgeline_infrastructure_management					
N/A	05-Aug-21	5	A potential security vulnerability has been identified in the HPE Edgeline Infrastructure Manager, also known as HPE Edgeline Infrastructure Management Software. The vulnerability could be remotely exploited to disclose sensitive information. HPE has made software updates available to resolve the vulnerability in the HPE Edgeline Infrastructure Manager (EIM).	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04180en_us	A-HP-EDGE-180821/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26586		
htmly					
htmly					
N/A	03-Aug-21	6.4	In htmly version 2.8.1, is vulnerable to an Arbitrary File Deletion on the local host when delete backup files. The vulnerability may allow a remote attacker to delete arbitrary know files on the host. **CVE ID : CVE-2021-36701**	N/A	A-HTM-HTML-180821/234
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	4.3	The "content" field in the "regular post" page of the "add content" menu under "dashboard" in htmly 2.8.1 has a storage cross site scripting (XSS) vulnerability. It allows remote attackers to send authenticated post-http requests to add / content and inject arbitrary web scripts or HTML through special content. **CVE ID : CVE-2021-36702**	N/A	A-HTM-HTML-180821/235
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	4.3	The "blog title" field in the "Settings" menu "config" page of "dashboard" in htmly 2.8.1 has a storage cross site scripting (XSS) vulnerability. It allows remote attackers to send an authenticated post HTTP request to admin/config and inject arbitrary web script or HTML through a special website name.	N/A	A-HTM-HTML-180821/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36703		
Huawei					
emui					
Improper Input Validation	02-Aug-21	7.8	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22445**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-EMUI-180821/237
Exposure of Resource to Wrong Sphere	02-Aug-21	7.8	There is an Information Disclosure Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22446**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-EMUI-180821/238
Improper Check for Unusual or Exceptional Conditions	02-Aug-21	7.8	There is an Improper Check for Unusual or Exceptional Conditions Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22447**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-EMUI-180821/239
magic_ui					
Integer Underflow (Wrap or Wraparound)	02-Aug-21	5	There is an Integer Underflow (Wrap or Wraparound) Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause DoS of Samgr. **CVE ID : CVE-2021-22379**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Aug-21	5	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause an infinite loop in DoS. **CVE ID : CVE-2021-22381**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/241
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Aug-21	6.8	There is an Information Disclosure Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to authentication bypass. **CVE ID : CVE-2021-22384**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/242
Improper Control of Dynamically-Managed Code Resources	02-Aug-21	7.5	There is an Improper Control of Dynamically Managing Code Resources Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to remotely execute commands. **CVE ID : CVE-2021-22387**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/243
Integer Overflow or Wraparound	02-Aug-21	7.5	There is an Integer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause certain codes to be executed. **CVE ID : CVE-2021-22388**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/244
Incorrect Authorization	02-Aug-21	7.5	There is a Permission Control Vulnerability in Huawei Smartphone.Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin	A-HUA-MAGI-180821/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may cause certain codes to be executed. **CVE ID : CVE-2021-22389**	/2021/6/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Aug-21	7.5	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause certain codes to be executed. **CVE ID : CVE-2021-22390**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/246
Incorrect Calculation of Buffer Size	02-Aug-21	5	There is an Incorrect Calculation of Buffer Size in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22391**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/247
Incorrect Calculation of Buffer Size	02-Aug-21	5	There is an Incorrect Calculation of Buffer Size in Huawei Smartphone.Successful exploitation of this vulnerability may cause verification bypass and directions to abnormal addresses. **CVE ID : CVE-2021-22392**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/248
Integer Overflow or Wraparound	02-Aug-21	5	There is an Integer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause random kernel address access.	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22412		
Out-of-bounds Write	02-Aug-21	5	There is an Integer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22413**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/250
Out-of-bounds Write	02-Aug-21	5	There is a Memory Buffer Errors Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22414**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/251
Incorrect Calculation of Buffer Size	02-Aug-21	5	There is an Incorrect Calculation of Buffer Size Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause kernel exceptions with the code. **CVE ID : CVE-2021-22415**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/252
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Aug-21	6.8	There is a Heap-based Buffer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to authentication bypass. **CVE ID : CVE-2021-22427**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/253
Concurrent Execution using Shared	02-Aug-21	6.8	There is an Incomplete Cleanup Vulnerability in Huawei	https://consumer.huawei.com/en/sup	A-HUA-MAGI-180821/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Smartphone.Successful exploitation of this vulnerability may lead to authentication bypass. **CVE ID : CVE-2021-22428**	port/bulletin/2021/6/	
N/A	02-Aug-21	6.4	There is a Configuration Defect Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service integrity and availability. **CVE ID : CVE-2021-22435**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/255
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Aug-21	7.5	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause malicious code to be executed. **CVE ID : CVE-2021-22438**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/256
Improper Validation of Integrity Check Value	02-Aug-21	5	There is an Improper Validation of Integrity Check Value Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22442**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/257
Improper Input Validation	02-Aug-21	5	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause random address access.	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22443		
Improper Input Validation	02-Aug-21	7.5	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause code injection. **CVE ID : CVE-2021-22444**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/259
Improper Input Validation	02-Aug-21	7.8	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22445**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/260
Exposure of Resource to Wrong Sphere	02-Aug-21	7.8	There is an Information Disclosure Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22446**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/261
Improper Check for Unusual or Exceptional Conditions	02-Aug-21	7.8	There is an Improper Check for Unusual or Exceptional Conditions Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22447**	https://consumer.huawei.com/en/support/bulletin/2021/6/	A-HUA-MAGI-180821/262
manageone					
Improper Privilege Management	02-Aug-21	4.6	There is a privilege escalation vulnerability in Huawei ManageOne 8.0.0. External	https://www.huawei.com/en/psirt/sec	A-HUA-MANA-180821/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameters of some files are lack of verification when they are be called. Attackers can exploit this vulnerability by performing these files to cause privilege escalation attack. This can compromise normal service. **CVE ID : CVE-2021-22397**	urity-advisories/huawei-sa-20210714-01-pe-en	
IBM					
cloud_pak_for_security					
Incorrect Authorization	02-Aug-21	5	IBM Cloud Pak for Security (CP4S) 1.5.0.0, 1.5.1.0, 1.6.0.0, 1.6.1.0, 1.7.0.0, and 1.7.1.0 could disclose sensitive information to an unauthorized user through HTTP GET requests. This information could be used in further attacks against the system. IBM X-Force ID: 198920. **CVE ID : CVE-2021-20539**	https://www.ibm.com/support/pages/node/6476940	A-IBM-CLOU-180821/264
Incorrect Authorization	02-Aug-21	5	IBM Cloud Pak for Security (CP4S) 1.5.0.0, 1.5.1.0, 1.6.0.0, 1.6.1.0, 1.7.0.0, and 1.7.1.0 could disclose sensitive information to an unauthorized user through HTTP GET requests. This information could be used in further attacks against the system. IBM X-Force ID: 198923. **CVE ID : CVE-2021-20540**	https://www.ibm.com/support/pages/node/6476940	A-IBM-CLOU-180821/265
Incorrect Authorizatio	02-Aug-21	5	IBM Cloud Pak for Security (CP4S) 1.5.0.0, 1.5.1.0, 1.6.0.0,	https://www.ibm.com/su	A-IBM-CLOU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			1.6.1.0, 1.7.0.0, and 1.7.1.0 could disclose sensitive information to an unauthorized user through HTTP GET requests. This information could be used in further attacks against the system. IBM X-Force ID: 198927. **CVE ID : CVE-2021-20541**	pport/pages/node/6476940	180821/266
N/A	02-Aug-21	9	IBM Cloud Pak for Security (CP4S) 1.5.0.0, 1.5.1.0, 1.6.0.0, 1.6.1.0, 1.7.0.0, and 1.7.1.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. **CVE ID : CVE-2021-29696**	https://www.ibm.com/support/pages/node/6476940, https://exchange.xforce.ibmcloud.com/vulnerabilities/200597	A-IBM-CLOU-180821/267
N/A	02-Aug-21	4	IBM Cloud Pak for Security (CP4S) 1.5.0.0, 1.5.1.0, 1.6.0.0, 1.6.1.0, 1.7.0.0, and 1.7.1.0 could allow a remote authenticated attacker to obtain sensitive information through HTTP requests that could be used in further attacks against the system. **CVE ID : CVE-2021-29697**	https://www.ibm.com/support/pages/node/6476940, https://exchange.xforce.ibmcloud.com/vulnerabilities/200598	A-IBM-CLOU-180821/268
qradar_user_behavior_analytics					
Cross-Site Request Forgery (CSRF)	02-Aug-21	6.8	IBM QRadar User Behavior Analytics 4.1.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that	https://www.ibm.com/support/pages/node/6477204	A-IBM-QRAD-180821/269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the website trusts. IBM X-Force ID: 202168. **CVE ID : CVE-2021-29757**		
Iobit					
advanced_systemcare_ultimate					
N/A	05-Aug-21	2.1	An information disclosure vulnerability exists in the IOCTL 0x9c40a148 handling of IOBit Advanced SystemCare Ultimate 14.2.0.220. A specially crafted I/O request packet (IRP) can lead to a disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2021-21785**	N/A	A-IOB-ADVA-180821/270
N/A	05-Aug-21	2.1	An information disclosure vulnerability exists in the the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O read requests. A specially crafted I/O request packet (IRP) can lead to privileged reads in the context of a driver which can result in sensitive information disclosure from the kernel. The IN instruction can read two bytes from the given I/O device, potentially leaking sensitive device data to unprivileged users. **CVE ID : CVE-2021-21790**	N/A	A-IOB-ADVA-180821/271
N/A	05-Aug-21	2.1	An information disclosure vulnerability exists in the the	N/A	A-IOB-ADVA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O read requests. A specially crafted I/O request packet (IRP) can lead to privileged reads in the context of a driver which can result in sensitive information disclosure from the kernel. The IN instruction can read two bytes from the given I/O device, potentially leaking sensitive device data to unprivileged users. **CVE ID : CVE-2021-21791**		180821/272
N/A	05-Aug-21	2.1	An information disclosure vulnerability exists in the the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O read requests. A specially crafted I/O request packet (IRP) can lead to privileged reads in the context of a driver which can result in sensitive information disclosure from the kernel. The IN instruction can read four bytes from the given I/O device, potentially leaking sensitive device data to unprivileged users. **CVE ID : CVE-2021-21792**	N/A	A-IOB-ADVA-180821/273
ipdgroup					
newsplugin					
Cross-Site Request	05-Aug-21	6.8	The NewsPlugin WordPress plugin is vulnerable to Cross-	N/A	A-IPD-NEWS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Site Request Forgery via the handle_save_style function found in the ~/news-plugin.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.18. **CVE ID : CVE-2021-34631**		180821/274
Jetbrains					
hub					
Weak Password Recovery Mechanism for Forgotten Password	06-Aug-21	7.5	In JetBrains Hub before 2021.1.13389, account takeover was possible during password reset. **CVE ID : CVE-2021-36209**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-HUB-180821/275
Inadequate Encryption Strength	06-Aug-21	6.4	In JetBrains Hub before 2021.1.13262, a potentially insufficient CSP for the Widget deployment feature was used. **CVE ID : CVE-2021-37540**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-HUB-180821/276
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-Aug-21	4.3	In JetBrains Hub before 2021.1.13402, HTML injection in the password reset email was possible. **CVE ID : CVE-2021-37541**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-HUB-180821/277
rubymine					
N/A	06-Aug-21	6.5	In JetBrains RubyMine before 2021.1.1, code execution without user confirmation	https://blog.jetbrains.com/blog/2021/	A-JET-RUBY-180821/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			was possible for untrusted projects. **CVE ID : CVE-2021-37543**	08/05/jetbrains-security-bulletin-q2-2021/	
teamcity					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-21	4.3	In JetBrains TeamCity before 2020.2.3, XSS was possible. **CVE ID : CVE-2021-37542**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-TEAM-180821/279
Deserialization of Untrusted Data	06-Aug-21	7.5	In JetBrains TeamCity before 2020.2.4, there was an insecure deserialization. **CVE ID : CVE-2021-37544**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-TEAM-180821/280
Improper Authentication	06-Aug-21	5	In JetBrains TeamCity before 2021.1.1, insufficient authentication checks for agent requests were made. **CVE ID : CVE-2021-37545**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-TEAM-180821/281
Inadequate Encryption Strength	06-Aug-21	5	In JetBrains TeamCity before 2021.1, an insecure key generation mechanism for encrypted properties was used. **CVE ID : CVE-2021-37546**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-TEAM-180821/282
N/A	06-Aug-21	5	In JetBrains TeamCity before 2020.2.4, insufficient checks during file uploading were	https://blog.jetbrains.com/blog/2021/08/05/jetbra	A-JET-TEAM-180821/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			made. **CVE ID : CVE-2021-37547**	ins-security-bulletin-q2-2021/	
Cleartext Storage of Sensitive Information	06-Aug-21	5	In JetBrains TeamCity before 2021.1, passwords in cleartext sometimes could be stored in VCS. **CVE ID : CVE-2021-37548**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-TEAM-180821/284
youtrack					
N/A	06-Aug-21	6.4	In JetBrains YouTrack before 2021.1.11111, sandboxing in workflows was insufficient. **CVE ID : CVE-2021-37549**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-YOUT-180821/285
Incorrect Comparison	06-Aug-21	5	In JetBrains YouTrack before 2021.2.16363, time-unsafe comparisons were used. **CVE ID : CVE-2021-37550**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-YOUT-180821/286
Inadequate Encryption Strength	06-Aug-21	5	In JetBrains YouTrack before 2021.2.16363, system user passwords were hashed with SHA-256. **CVE ID : CVE-2021-37551**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-YOUT-180821/287
Improper Neutralization of Input During Web Page Generation	06-Aug-21	3.5	In JetBrains YouTrack before 2021.2.17925, stored XSS was possible. **CVE ID : CVE-2021-37552**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-	A-JET-YOUT-180821/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				2021/	
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	06-Aug-21	5	In JetBrains YouTrack before 2021.2.16363, an insecure PRNG was used. **CVE ID : CVE-2021-37553**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-YOUT-180821/289
Exposure of Sensitive Information to an Unauthorized Actor	06-Aug-21	4	In JetBrains YouTrack before 2021.3.21051, a user could see boards without having corresponding permissions. **CVE ID : CVE-2021-37554**	https://blog.jetbrains.com/blog/2021/08/05/jetbrains-security-bulletin-q2-2021/	A-JET-YOUT-180821/290
joplin_project					
joplin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	4.3	Joplin before 2.0.9 allows XSS via button and form in the note body. **CVE ID : CVE-2021-37916**	https://github.com/laurent22/joplin/commit/feaecf765368f2c273bea3a9fa641ff0da7e6b26	A-JOP-JOPL-180821/291
jump-technology					
asset_management					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-21	6.5	An issue was discovered in JUMP AMS 3.6.0.04.009-2487. A JUMP SOAP endpoint permitted the writing of arbitrary files to a user-controlled location on the remote filesystem (with user-controlled content) via	N/A	A-JUM-ASSE-180821/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			directory traversal, potentially leading to remote code and command execution. **CVE ID : CVE-2021-32016**		
N/A	03-Aug-21	4	An issue was discovered in JUMP AMS 3.6.0.04.009-2487. A JUMP SOAP endpoint permitted the listing of the content of the remote file system. This can be used to identify the complete server filesystem structure, i.e., identifying all the directories and files. **CVE ID : CVE-2021-32017**	N/A	A-JUM-ASSE-180821/293
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-21	4	An issue was discovered in JUMP AMS 3.6.0.04.009-2487. The JUMP SOAP API was vulnerable to arbitrary file reading due to an improper limitation of file loading on the server filesystem, aka directory traversal. **CVE ID : CVE-2021-32018**	N/A	A-JUM-ASSE-180821/294
kainelabs					
youzify					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The About Me widget of the Youzify â€“ BuddyPress Community, User Profile, Social Network & Membership WordPress plugin before 1.0.7 does not properly sanitise its Biography field, allowing any authenticated user to set Cross-Site Scripting payloads in it, which will be executed	N/A	A-KAI-YOUZ-180821/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when viewing the affected user profile. This could allow a low privilege user to gain unauthorised access to the admin side of the blog by targeting an admin, inducing them to view their profile with a malicious payload adding a rogue account for example. **CVE ID : CVE-2021-24443**		
kentharadio_project					
kentharadio					
Server-Side Request Forgery (SSRF)	02-Aug-21	7.5	The OnAir2 WordPress theme before 3.9.9.2 and QT KenthaRadio WordPress plugin before 2.0.2 have exposed proxy functionality to unauthenticated users, sending requests to this proxy functionality will have the web server fetch and display the content from any URI, this would allow for SSRF (Server Side Request Forgery) and RFI (Remote File Inclusion) vulnerabilities on the website. **CVE ID : CVE-2021-24472**	N/A	A-KEN-KENT-180821/296
lancer_project					
lancer					
Integer Overflow or Wraparound	03-Aug-21	5	An integer overflow in the transfer function of a smart contract implementation for Lancer Token, an Ethereum ERC20 token, allows the owner to cause unexpected financial losses between two	N/A	A-LAN-LANC-180821/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			large accounts during a transaction. **CVE ID : CVE-2021-33403**		
leostream					
connection_broker					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-21	4.3	** UNSUPPORTED WHEN ASSIGNED ** LeoStream Connection Broker 9.x before 9.0.34.3 allows Unauthenticated Reflected XSS via the /index.pl user parameter. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2021-38157**	https://www.leostream.com/resources-2/product-lifecycle/, https://leostream.com	A-LEO-CONN-180821/298
Libgd					
libgd					
Out-of-bounds Read	04-Aug-21	4.3	read_header_tga in gd_tga.c in the GD Graphics Library (aka LibGD) through 2.3.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA file. **CVE ID : CVE-2021-38115**	https://github.com/libgd/libgd/pull/711/commits/8b111b2b4a4842179be66db68d84dda91a246032	A-LIB-LIBG-180821/299
Liferay					
dxp					
Allocation of Resources Without Limits or Throttling	03-Aug-21	4	The Flags module in Liferay Portal 7.3.1 and earlier, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 20, and 7.2 before fix pack 5, does not limit the rate at which content can be flagged as inappropriate, which	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mx	A-LIF-DXP-180821/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows remote authenticated users to spam the site administrator with emails **CVE ID : CVE-2021-33320**	mVrnXW/content/id/120747590, https://issues.liferay.com/browse/LPE-17007	
Weak Password Recovery Mechanism for Forgotten Password	03-Aug-21	5	Insecure default configuration in Liferay Portal 6.2.3 through 7.3.2, and Liferay DXP before 7.3, allows remote attackers to enumerate user email address via the forgot password functionality. The portal.property login.secure.forgot.password should be defaulted to true. **CVE ID : CVE-2021-33321**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120748055, https://help.liferay.com/hc/en-us/articles/360050785632	A-LIF-DXP-180821/301
Insufficient Session Expiration	03-Aug-21	5	In Liferay Portal 7.3.0 and earlier, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 18, and 7.2 before fix pack 5, password reset tokens are not invalidated after a user changes their password, which allows remote attackers to change the user's password via the old password reset token. **CVE ID : CVE-2021-33322**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120748020, https://issues.liferay.com/browse/LPE-16981	A-LIF-DXP-180821/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	03-Aug-21	5	The Dynamic Data Mapping module in Liferay Portal 7.1.0 through 7.3.2, and Liferay DXP 7.1 before fix pack 19, and 7.2 before fix pack 7, autosaves form values for unauthenticated users, which allows remote attackers to view the autosaved values by viewing the form as an unauthenticated user. **CVE ID : CVE-2021-33323**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747107, https://issues.liferay.com/browse/LPE-17049	A-LIF-DXP-180821/303
Incorrect Default Permissions	03-Aug-21	4	The Layout module in Liferay Portal 7.1.0 through 7.3.1, and Liferay DXP 7.1 before fix pack 20, and 7.2 before fix pack 5, does not properly check permission of pages, which allows remote authenticated users without view permission of a page to view the page via a site's page administration. **CVE ID : CVE-2021-33324**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747063, https://issues.liferay.com/browse/LPE-17001	A-LIF-DXP-180821/304
Cleartext Storage of Sensitive Information	03-Aug-21	4	The Portal Workflow module in Liferay Portal 7.3.2 and earlier, and Liferay DXP 7.0 before fix pack 93, 7.1 before fix pack 19, and 7.2 before fix pack 7, user's clear text passwords are stored in the database if workflow is enabled for user creation,	https://issues.liferay.com/browse/LPE-17042, https://portal.liferay.dev/learn/security/known-vulnerabilitie	A-LIF-DXP-180821/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which allows attackers with access to the database to obtain a user's password. **CVE ID : CVE-2021-33325**	s/-/asset_publisher/HbL5mxmVrnXW/content/id/120748389	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	4.3	Cross-site scripting (XSS) vulnerability in the Frontend JS module in Liferay Portal 7.3.4 and earlier, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 20 and 7.2 before fix pack 9, allows remote attackers to inject arbitrary web script or HTML via the title of a modal window. **CVE ID : CVE-2021-33326**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747869, https://issues.liferay.com/browse/LPE-17093	A-LIF-DXP-180821/306
Incorrect Default Permissions	03-Aug-21	4	The Portlet Configuration module in Liferay Portal 7.2.0 through 7.3.3, and Liferay DXP 7.0 fix pack pack 93 and 94, 7.1 fix pack 18, and 7.2 before fix pack 8, does not properly check user permission, which allows remote authenticated users to view the Guest and User role even if "Role Visibility" is enabled. **CVE ID : CVE-2021-33327**	https://issues.liferay.com/browse/LPE-17075, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747840	A-LIF-DXP-180821/307
Improper Neutralization of Input	03-Aug-21	3.5	Cross-site scripting (XSS) vulnerability in the Asset module's edit vocabulary	https://issues.liferay.com/browse/LPE	A-LIF-DXP-180821/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			page in Liferay Portal 7.0.0 through 7.3.4, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 20, and 7.2 before fix pack 9, allows remote attackers to inject arbitrary web script or HTML via the (1) _com_liferay_journal_web_portlet_JournalPortlet_name or (2) _com_liferay_document_library_web_portlet_DLAdminPortlet_name parameter. **CVE ID : CVE-2021-33328**	-17100, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747972	
Exposure of Resource to Wrong Sphere	03-Aug-21	4.3	Liferay Portal 7.2.0 through 7.3.2, and Liferay DXP 7.2 before fix pack 9, allows access to Cross-origin resource sharing (CORS) protected resources if the user is only authenticated using the portal session authentication, which allows remote attackers to obtain sensitive information including the targeted user's email address and current CSRF token. **CVE ID : CVE-2021-33330**	https://issues.liferay.com/browse/LPE-17127, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747720	A-LIF-DXP-180821/309
URL Redirection to Untrusted Site ('Open Redirect')	03-Aug-21	5.8	Open redirect vulnerability in the Notifications module in Liferay Portal 7.0.0 through 7.3.1, and Liferay DXP 7.0 before fix pack 94, 7.1 before fix pack 19 and 7.2 before fix pack 8, allows remote attackers to redirect users to	https://issues.liferay.com/browse/LPE-17022, https://portal.liferay.dev/learn/security/known-	A-LIF-DXP-180821/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary external URLs via the 'redirect' parameter. **CVE ID : CVE-2021-33331**	vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747627	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	4.3	Cross-site scripting (XSS) vulnerability in the Portlet Configuration module in Liferay Portal 7.1.0 through 7.3.2, and Liferay DXP 7.1 before fix pack 19, and 7.2 before fix pack 7, allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_portlet_configuration_css_web_portlet_PortletConfigurationCSSPortlet_portletResource parameter. **CVE ID : CVE-2021-33332**	https://issues.liferay.com/browse/LPE-17053, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120748366	A-LIF-DXP-180821/311
Incorrect Default Permissions	03-Aug-21	6.5	The Portal Workflow module in Liferay Portal 7.3.2 and earlier, and Liferay DXP 7.0 before fix pack 93, 7.1 before fix pack 19 and 7.2 before fix pack 6, does not properly check user permission, which allows remote authenticated users to view and delete workflow submissions via crafted URLs. **CVE ID : CVE-2021-33333**	https://issues.liferay.com/browse/LPE-17032, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747742	A-LIF-DXP-180821/312
Incorrect	03-Aug-21	4	The Dynamic Data Mapping	https://issue	A-LIF-DXP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			module in Liferay Portal 7.0.0 through 7.3.2, and Liferay DXP 7.0 before fix pack 94, 7.1 before fix pack 19, and 7.2 before fix pack 6, does not properly check user permissions, which allows remote attackers with the forms "Access in Site Administration" permission to view all forms and form entries in a site via the forms section in site administration. **CVE ID : CVE-2021-33334**	s.liferay.com/browse/LPE-17039, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120748332	180821/313
Improper Privilege Management	03-Aug-21	6.5	Privilege escalation vulnerability in Liferay Portal 7.0.3 through 7.3.4, and Liferay DXP 7.1 before fix pack 20, and 7.2 before fix pack 9 allows remote authenticated users with permission to update/edit users to take over a company administrator user account by editing the company administrator user. **CVE ID : CVE-2021-33335**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747906, https://issues.liferay.com/browse/LPE-17103	A-LIF-DXP-180821/314
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	3.5	Cross-site scripting (XSS) vulnerability in the Journal module's add article menu in Liferay Portal 7.3.0 through 7.3.3, and Liferay DXP 7.1 fix pack 18, and 7.2 fix pack 5 through 7, allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_journal_web_por	https://issues.liferay.com/browse/LPE-17078, https://portal.liferay.dev/learn/security/known-vulnerabilities/-	A-LIF-DXP-180821/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tlet_JournalPortlet_name parameter. **CVE ID : CVE-2021-33336**	/asset_publisher/HbL5mxmVrnXW/content/cve-2021-33336-stored-xss-with-structure-name	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	4.3	Cross-site scripting (XSS) vulnerability in the Document Library module's add document menu in Liferay Portal 7.3.0 through 7.3.4, and Liferay DXP 7.1 before fix pack 20, and 7.2 before fix pack 9, allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_document_library_web_portlet_DLAdminPortlet_name parameter. **CVE ID : CVE-2021-33337**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2021-33337-stored-xss-with-document-types-in-documents-and-media, https://issues.liferay.com/browse/LPE-17101	A-LIF-DXP-180821/316
Cross-Site Request Forgery (CSRF)	04-Aug-21	5.1	The Layout module in Liferay Portal 7.1.0 through 7.3.2, and Liferay DXP 7.1 before fix pack 19, and 7.2 before fix pack 6, exposes the CSRF token in URLs, which allows man-in-the-middle attackers to obtain the token and conduct Cross-Site Request	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/co	A-LIF-DXP-180821/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Forgery (CSRF) attacks via the p_auth parameter. **CVE ID : CVE-2021-33338**	ntent/id/120748276, https://issues.liferay.com/browse/LPE-17030	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	3.5	Cross-site scripting (XSS) vulnerability in the Fragment module in Liferay Portal 7.2.1 through 7.3.4, and Liferay DXP 7.2 before fix pack 9 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_site_admin_web_portlet_SiteAdminPortlet_name parameter. **CVE ID : CVE-2021-33339**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747934, https://issues.liferay.com/browse/LPE-17102	A-LIF-DXP-180821/318
liferay_portal					
Allocation of Resources Without Limits or Throttling	03-Aug-21	4	The Flags module in Liferay Portal 7.3.1 and earlier, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 20, and 7.2 before fix pack 5, does not limit the rate at which content can be flagged as inappropriate, which allows remote authenticated users to spam the site administrator with emails **CVE ID : CVE-2021-33320**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747590, https://issues.liferay.com/browse/LPE-17007	A-LIF-LIFE-180821/319
Weak	03-Aug-21	5	Insecure default configuration	https://porta	A-LIF-LIFE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Password Recovery Mechanism for Forgotten Password			in Liferay Portal 6.2.3 through 7.3.2, and Liferay DXP before 7.3, allows remote attackers to enumerate user email address via the forgot password functionality. The portal.property login.secure.forgot.password should be defaulted to true. **CVE ID : CVE-2021-33321**	l.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120748055, https://help.liferay.com/hc/en-us/articles/360050785632	180821/320
Insufficient Session Expiration	03-Aug-21	5	In Liferay Portal 7.3.0 and earlier, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 18, and 7.2 before fix pack 5, password reset tokens are not invalidated after a user changes their password, which allows remote attackers to change the user's password via the old password reset token. **CVE ID : CVE-2021-33322**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120748020, https://issues.liferay.com/browse/LPE-16981	A-LIF-LIFE-180821/321
Cleartext Storage of Sensitive Information	03-Aug-21	5	The Dynamic Data Mapping module in Liferay Portal 7.1.0 through 7.3.2, and Liferay DXP 7.1 before fix pack 19, and 7.2 before fix pack 7, autosaves form values for unauthenticated users, which allows remote attackers to	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mx	A-LIF-LIFE-180821/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			view the autosaved values by viewing the form as an unauthenticated user. **CVE ID : CVE-2021-33323**	mVrnXW/content/id/120747107, https://issues.liferay.com/browse/LPE-17049	
Incorrect Default Permissions	03-Aug-21	4	The Layout module in Liferay Portal 7.1.0 through 7.3.1, and Liferay DXP 7.1 before fix pack 20, and 7.2 before fix pack 5, does not properly check permission of pages, which allows remote authenticated users without view permission of a page to view the page via a site's page administration. **CVE ID : CVE-2021-33324**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747063, https://issues.liferay.com/browse/LPE-17001	A-LIF-LIFE-180821/323
Cleartext Storage of Sensitive Information	03-Aug-21	4	The Portal Workflow module in Liferay Portal 7.3.2 and earlier, and Liferay DXP 7.0 before fix pack 93, 7.1 before fix pack 19, and 7.2 before fix pack 7, user's clear text passwords are stored in the database if workflow is enabled for user creation, which allows attackers with access to the database to obtain a user's password. **CVE ID : CVE-2021-33325**	https://issues.liferay.com/browse/LPE-17042, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120748389	A-LIF-LIFE-180821/324
Improper Neutralizatio	03-Aug-21	4.3	Cross-site scripting (XSS) vulnerability in the Frontend	https://portal.liferay.dev/l	A-LIF-LIFE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			JS module in Liferay Portal 7.3.4 and earlier, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 20 and 7.2 before fix pack 9, allows remote attackers to inject arbitrary web script or HTML via the title of a modal window. **CVE ID : CVE-2021-33326**	earn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747869, https://issues.liferay.com/browse/LPE-17093	180821/325
Incorrect Default Permissions	03-Aug-21	4	The Portlet Configuration module in Liferay Portal 7.2.0 through 7.3.3, and Liferay DXP 7.0 fix pack pack 93 and 94, 7.1 fix pack 18, and 7.2 before fix pack 8, does not properly check user permission, which allows remote authenticated users to view the Guest and User role even if "Role Visibility" is enabled. **CVE ID : CVE-2021-33327**	https://issues.liferay.com/browse/LPE-17075, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747840	A-LIF-LIFE-180821/326
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	3.5	Cross-site scripting (XSS) vulnerability in the Asset module's edit vocabulary page in Liferay Portal 7.0.0 through 7.3.4, and Liferay DXP 7.0 before fix pack 96, 7.1 before fix pack 20, and 7.2 before fix pack 9, allows remote attackers to inject arbitrary web script or HTML via the (1)	https://issues.liferay.com/browse/LPE-17100, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publis	A-LIF-LIFE-180821/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			_com_liferay_journal_web_portlet_JournalPortlet_name or (2) _com_liferay_document_library_web_portlet_DLAdminPortlet_name parameter. **CVE ID : CVE-2021-33328**	her/HbL5mxmVrnXW/content/id/120747972	
Exposure of Resource to Wrong Sphere	03-Aug-21	4.3	Liferay Portal 7.2.0 through 7.3.2, and Liferay DXP 7.2 before fix pack 9, allows access to Cross-origin resource sharing (CORS) protected resources if the user is only authenticated using the portal session authentication, which allows remote attackers to obtain sensitive information including the targeted user's email address and current CSRF token. **CVE ID : CVE-2021-33330**	https://issues.liferay.com/browse/LPE-17127, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747720	A-LIF-LIFE-180821/328
URL Redirection to Untrusted Site ('Open Redirect')	03-Aug-21	5.8	Open redirect vulnerability in the Notifications module in Liferay Portal 7.0.0 through 7.3.1, and Liferay DXP 7.0 before fix pack 94, 7.1 before fix pack 19 and 7.2 before fix pack 8, allows remote attackers to redirect users to arbitrary external URLs via the 'redirect' parameter. **CVE ID : CVE-2021-33331**	https://issues.liferay.com/browse/LPE-17022, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747627	A-LIF-LIFE-180821/329
Improper	03-Aug-21	4.3	Cross-site scripting (XSS)	https://issue	A-LIF-LIFE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			vulnerability in the Portlet Configuration module in Liferay Portal 7.1.0 through 7.3.2, and Liferay DXP 7.1 before fix pack 19, and 7.2 before fix pack 7, allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_portlet_configuration_css_web_portlet_PortletConfigurationCSSPortlet_portletResource parameter. **CVE ID : CVE-2021-33332**	s.liferay.com/browse/LPE-17053, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120748366	180821/330
Incorrect Default Permissions	03-Aug-21	6.5	The Portal Workflow module in Liferay Portal 7.3.2 and earlier, and Liferay DXP 7.0 before fix pack 93, 7.1 before fix pack 19 and 7.2 before fix pack 6, does not properly check user permission, which allows remote authenticated users to view and delete workflow submissions via crafted URLs. **CVE ID : CVE-2021-33333**	https://issues.liferay.com/browse/LPE-17032, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747742	A-LIF-LIFE-180821/331
Incorrect Default Permissions	03-Aug-21	4	The Dynamic Data Mapping module in Liferay Portal 7.0.0 through 7.3.2, and Liferay DXP 7.0 before fix pack 94, 7.1 before fix pack 19, and 7.2 before fix pack 6, does not properly check user permissions, which allows remote attackers with the forms "Access in Site	https://issues.liferay.com/browse/LPE-17039, https://portal.liferay.dev/learn/security/known-vulnerabilities/-	A-LIF-LIFE-180821/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Administration" permission to view all forms and form entries in a site via the forms section in site administration. **CVE ID : CVE-2021-33334**	/asset_publisher/HbL5mxmVrnXW/content/id/120748332	
Improper Privilege Management	03-Aug-21	6.5	Privilege escalation vulnerability in Liferay Portal 7.0.3 through 7.3.4, and Liferay DXP 7.1 before fix pack 20, and 7.2 before fix pack 9 allows remote authenticated users with permission to update/edit users to take over a company administrator user account by editing the company administrator user. **CVE ID : CVE-2021-33335**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747906, https://issues.liferay.com/browse/LPE-17103	A-LIF-LIFE-180821/333
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	3.5	Cross-site scripting (XSS) vulnerability in the Journal module's add article menu in Liferay Portal 7.3.0 through 7.3.3, and Liferay DXP 7.1 fix pack 18, and 7.2 fix pack 5 through 7, allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_journal_web_portlet_JournalPortlet_name parameter. **CVE ID : CVE-2021-33336**	https://issues.liferay.com/browse/LPE-17078, https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2021-33336-stored-xss-with-structure-	A-LIF-LIFE-180821/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				name	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	4.3	Cross-site scripting (XSS) vulnerability in the Document Library module's add document menu in Liferay Portal 7.3.0 through 7.3.4, and Liferay DXP 7.1 before fix pack 20, and 7.2 before fix pack 9, allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_document_library_web_portlet_DLAdminPortlet_name parameter. **CVE ID : CVE-2021-33337**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2021-33337-stored-xss-with-document-types-in-documents-and-media, https://issues.liferay.com/browse/LPE-17101	A-LIF-LIFE-180821/335
Cross-Site Request Forgery (CSRF)	04-Aug-21	5.1	The Layout module in Liferay Portal 7.1.0 through 7.3.2, and Liferay DXP 7.1 before fix pack 19, and 7.2 before fix pack 6, exposes the CSRF token in URLs, which allows man-in-the-middle attackers to obtain the token and conduct Cross-Site Request Forgery (CSRF) attacks via the p_auth parameter. **CVE ID : CVE-2021-33338**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120748276, https://issues.liferay.com/browse/LPE-17030	A-LIF-LIFE-180821/336
Improper Neutralizatio	04-Aug-21	3.5	Cross-site scripting (XSS) vulnerability in the Fragment	https://portal.liferay.dev/l	A-LIF-LIFE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			module in Liferay Portal 7.2.1 through 7.3.4, and Liferay DXP 7.2 before fix pack 9 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_site_admin_web_portlet_SiteAdminPortlet_name parameter. **CVE ID : CVE-2021-33339**	earn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120747934, https://issues.liferay.com/browse/LPE-17102	180821/337
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	4.3	Cross-site scripting (XSS) vulnerability in the Frontend Taglib module in Liferay Portal 7.4.0 allows remote attackers to inject arbitrary web script or HTML into the management toolbar search via the `keywords` parameter. **CVE ID : CVE-2021-35463**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/120850663	A-LIF-LIFE-180821/338
Linuxfoundation					
cortex					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-21	5	An issue was discovered in Grafana Cortex through 1.9.0. The header value X-Scope-OrgID is used to construct file paths for rules files, and if crafted to conduct directory traversal such as ae ../../sensitive/path/in/deployment pathname, then Cortex will attempt to parse a rules file at that location and include some of the contents	https://github.com/cortexproject/cortex/pull/4375, https://grafana.com/docs/grafana/latest/release-notes/	A-LIN-CORT-180821/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the error message. (Other Cortex API requests can also be sent a malicious OrgID header, e.g., tricking the ingester into writing metrics to a different location, but the effect is nuisance rather than information disclosure.) **CVE ID : CVE-2021-36157**		
lynx_project					
lynx					
Insufficiently Protected Credentials	07-Aug-21	5	Lynx through 2.8.9 mishandles the userinfo subcomponent of a URI, which allows remote attackers to discover cleartext credentials because they may appear in SNI data. **CVE ID : CVE-2021-38165**	N/A	A-LYN-LYNX-180821/340
mattermost					
mattermost					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-21	4.3	Fixed a bypass for a reflected cross-site scripting vulnerability affecting OAuth-enabled instances of Mattermost. **CVE ID : CVE-2021-37859**	https://mattermost.com/security-updates/	A-MAT-MATT-180821/341
Maxsite					
maxsite_cms					
Improper Neutralization of Input During Web Page	03-Aug-21	4.3	A reflected cross-site scripting (XSS) vulnerability in MaxSite CMS before V106 via product/page/* allows remote attackers to inject	https://github.com/maxsite/cms/commit/6b0ab1de9f3d471485	A-MAX-MAXS-180821/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			arbitrary web script to a page. **CVE ID : CVE-2021-35265**	d1347e800a 9ce43fedbf1a	
mbconnectline					
mbconnect24					
Incorrect Resource Transfer Between Spheres	02-Aug-21	4	In MB connect line mymbCONNECT24, mbCONNECT24 in versions <= 2.8.0 an authenticated attacker can change the password of his account into a new password that violates the password policy by intercepting and modifying the request that is send to the server. **CVE ID : CVE-2021-34574**	https://cert.vde.com/de-de/advisories/vde-2021-030	A-MBC-MBCO-180821/343
Observable Discrepancy	02-Aug-21	5	In MB connect line mymbCONNECT24, mbCONNECT24 in versions <= 2.8.0 an unauthenticated user can enumerate valid users by checking what kind of response the server sends. **CVE ID : CVE-2021-34575**	https://cert.vde.com/de-de/advisories/vde-2021-030	A-MBC-MBCO-180821/344
mbdialup					
Improper Privilege Management	02-Aug-21	7.2	In MB connect line mbDIALUP versions <= 3.9R0.0 a low privileged local attacker can send a command to the service running with NT AUTHORITY\SYSTEM instructing it to execute a malicous OpenVPN configuration resulting in arbitrary code execution with the privileges of the service.	https://cert.vde.com/de-de/advisories/vde-2021-017	A-MBC-MBDI-180821/345

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-2021-33526		
Improper Input Validation	02-Aug-21	7.2	In MB connect line mbDIALUP versions <= 3.9R0.0 a low privileged local attacker can send a command to the service running with NT AUTHORITY\SYSTEM that won't be validated correctly and allows for an arbitrary code execution with the privileges of the service. **CVE ID : CVE-2021-33527**	https://cert.vde.com/de-de/advisories/vde-2021-017	A-MBC-MBDI-180821/346
mymbconnect24					
Incorrect Resource Transfer Between Spheres	02-Aug-21	4	In MB connect line mymbCONNECT24, mbCONNECT24 in versions <= 2.8.0 an authenticated attacker can change the password of his account into a new password that violates the password policy by intercepting and modifying the request that is send to the server. **CVE ID : CVE-2021-34574**	https://cert.vde.com/de-de/advisories/vde-2021-030	A-MBC-MYMB-180821/347
Observable Discrepancy	02-Aug-21	5	In MB connect line mymbCONNECT24, mbCONNECT24 in versions <= 2.8.0 an unauthenticated user can enumerate valid users by checking what kind of response the server sends. **CVE ID : CVE-2021-34575**	https://cert.vde.com/de-de/advisories/vde-2021-030	A-MBC-MYMB-180821/348
Microchip					
miwi					
Incorrect	05-Aug-21	5	In the Microchip MiWi v6.5	https://www	A-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			software stack, there is a possibility of frame counters being validated/updated prior to message authentication. **CVE ID : CVE-2021-37604**	.microchip.com/product-change-notifications/#/, https://www.microchip.com/en-us/development-tools-tools-and-software/libraries-code-examples-and-more/advanced-software-framework-for-sam-devices#Downloads	MIWI-180821/349
Incorrect Authorization	05-Aug-21	5	In the Microchip MiWi v6.5 software stack, there is a possibility of frame counters being being validated / updated prior to message authentication. **CVE ID : CVE-2021-37605**	https://www.microchip.com/product-change-notifications/#/, https://www.microchip.com/en-us/development-tools-tools-and-software/libraries-code-examples-and-more/advanced-software-	A-MIC-MIWI-180821/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				framework-for-sam-devices#Downloads	
Microfocus					
data_protector					
Improper Privilege Management	05-Aug-21	6.5	A potential unauthorized privilege escalation vulnerability has been identified in Micro Focus Data Protector. The vulnerability affects versions 10.10, 10.20, 10.30, 10.40, 10.50, 10.60, 10.70, 10.80, 10.0 and 10.91. A privileged user may potentially misuse this feature and thus allow unintended and unauthorized access of data. **CVE ID : CVE-2021-22517**	https://portal.microfocus.com/s/article/KM000001460	A-MIC-DATA-180821/351
migrate_users_project					
migrate_users					
Cross-Site Request Forgery (CSRF)	02-Aug-21	4.3	The Migrate Users WordPress plugin through 1.0.1 does not sanitise or escape its Delimiter option before outputting in a page, leading to a Stored Cross-Site Scripting issue. Furthermore, the plugin does not have CSRF check in place when saving its options, allowing the issue to be exploited via a CSRF attack. **CVE ID : CVE-2021-24477**	N/A	A-MIG-MIGR-180821/352
Mongodb					
rust_driver					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Aug-21	2.1	Specific MongoDB Rust Driver versions can include credentials used by the connection pool to authenticate connections in the monitoring event that is emitted when the pool is created. The user's logging infrastructure could then potentially ingest these events and unexpectedly leak the credentials. Note that such monitoring is not enabled by default. **CVE ID : CVE-2021-20332**	https://jira.mongodb.org/browse/RUST-591	A-MON-RUST-180821/353
Mozilla					
firefox					
Use After Free	05-Aug-21	5.1	A malicious webpage could have triggered a use-after-free, memory corruption, and a potentially exploitable crash. *This bug could only be triggered when accessibility was enabled.*. This vulnerability affects Thunderbird < 78.12, Firefox ESR < 78.12, and Firefox < 90. **CVE ID : CVE-2021-29970**	https://www.mozilla.org/security/advisories/mfsa2021-30/, https://www.mozilla.org/security/advisories/mfsa2021-29/, https://www.mozilla.org/security/advisories/mfsa2021-28/	A-MOZ-FIRE-180821/354
Improper Preservation of Permissions	05-Aug-21	7.5	If a user had granted a permission to a webpage and saved that grant, any webpage running on the same host - irrespective of scheme or port - would be granted that	https://www.mozilla.org/security/advisories/mfsa2021-28/	A-MOZ-FIRE-180821/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permission. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 90. **CVE ID : CVE-2021-29971**		
Use After Free	05-Aug-21	6.8	A use-after-free vulnerability was found via testing, and traced to an out-of-date Cairo library. Updating the library resolved the issue, and may have remediated other, unknown security vulnerabilities as well. This vulnerability affects Firefox < 90. **CVE ID : CVE-2021-29972**	https://www.mozilla.org/security/advisories/mfsa2021-28/	A-MOZ-FIRE-180821/356
N/A	05-Aug-21	6.8	Password autofill was enabled without user interaction on insecure websites on Firefox for Android. This was corrected to require user interaction with the page before a user's password would be entered by the browser's autofill functionality *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 90. **CVE ID : CVE-2021-29973**	https://www.mozilla.org/security/advisories/mfsa2021-28/	A-MOZ-FIRE-180821/357
N/A	05-Aug-21	2.6	When network partitioning was enabled, e.g. as a result of Enhanced Tracking Protection settings, a TLS error page	https://www.mozilla.org/security/advisories/mfsa2	A-MOZ-FIRE-180821/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would allow the user to override an error on a domain which had specified HTTP Strict Transport Security (which implies that the error should not be override-able.) This issue did not affect the network connections, and they were correctly upgraded to HTTPS automatically. This vulnerability affects Firefox < 90. **CVE ID : CVE-2021-29974**	021-28/	
N/A	05-Aug-21	4.3	Through a series of DOM manipulations, a message, over which the attacker had control of the text but not HTML or formatting, could be overlaid on top of another domain (with the new domain correctly shown in the address bar) resulting in possible user confusion. This vulnerability affects Firefox < 90. **CVE ID : CVE-2021-29975**	https://www.mozilla.org/security/advisories/mfsa2021-28/	A-MOZ-FIRE-180821/359
Out-of-bounds Write	05-Aug-21	6.8	Mozilla developers reported memory safety bugs present in code shared between Firefox and Thunderbird. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.12,	https://www.mozilla.org/security/advisories/mfsa2021-30/, https://www.mozilla.org/security/advisories/mfsa2021-29/, https://www.mozilla.org/	A-MOZ-FIRE-180821/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 78.12, and Firefox < 90. **CVE ID : CVE-2021-29976**	security/advisories/mfsa2021-28/	
Out-of-bounds Write	05-Aug-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 89. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 90. **CVE ID : CVE-2021-29977**	https://www.mozilla.org/security/advisories/mfsa2021-28/	A-MOZ-FIRE-180821/361
firefox_esr					
Use After Free	05-Aug-21	5.1	A malicious webpage could have triggered a use-after-free, memory corruption, and a potentially exploitable crash. *This bug could only be triggered when accessibility was enabled.*. This vulnerability affects Thunderbird < 78.12, Firefox ESR < 78.12, and Firefox < 90. **CVE ID : CVE-2021-29970**	https://www.mozilla.org/security/advisories/mfsa2021-30/, https://www.mozilla.org/security/advisories/mfsa2021-29/, https://www.mozilla.org/security/advisories/mfsa2021-28/	A-MOZ-FIRE-180821/362
Out-of-bounds Write	05-Aug-21	6.8	Mozilla developers reported memory safety bugs present in code shared between Firefox and Thunderbird. Some of these bugs showed evidence of memory corruption and we presume	https://www.mozilla.org/security/advisories/mfsa2021-30/, https://www.mozilla.org/	A-MOZ-FIRE-180821/363

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
			that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.12, Firefox ESR < 78.12, and Firefox < 90. **CVE ID : CVE-2021-29976**	security/advisories/mfsa2021-29/, https://www.mozilla.org/security/advisories/mfsa2021-28/	
hubs_cloud					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	4.3	Hubs Cloud allows users to download shared content, specifically HTML and JS, which could allow javascript execution in the Hub Cloud instance's primary hosting domain.*. This vulnerability affects Hubs Cloud < mozillareality/reticulum/1.0.1/20210618012634. **CVE ID : CVE-2021-29979**	https://www.mozilla.org/security/advisories/mfsa2021-32/	A-MOZ-HUBS-180821/364
mozilla_vpn					
N/A	05-Aug-21	10	Multiple low security issues were discovered and fixed in a security audit of Mozilla VPN 2.x branch as part of a 3rd party security audit. This vulnerability affects Mozilla VPN < 2.3. **CVE ID : CVE-2021-29978**	https://github.com/mozilla-mobile/mozilla-vpn-client/pull/816, https://www.mozilla.org/security/advisories/mfsa2021-31/	A-MOZ-MOZI-180821/365
thunderbird					
Files or Directories Accessible to	05-Aug-21	4.3	If Thunderbird was configured to use STARTTLS for an IMAP connection, and	https://www.mozilla.org/security/advi	A-MOZ-THUN-180821/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
External Parties			an attacker injected IMAP server responses prior to the completion of the STARTTLS handshake, then Thunderbird didn't ignore the injected data. This could have resulted in Thunderbird showing incorrect information, for example the attacker could have tricked Thunderbird to show folders that didn't exist on the IMAP server. This vulnerability affects Thunderbird < 78.12. **CVE ID : CVE-2021-29969**	sories/mfsa2021-30/, https://bugzilla.mozilla.org/show_bug.cgi?id=1682370	
Use After Free	05-Aug-21	5.1	A malicious webpage could have triggered a use-after-free, memory corruption, and a potentially exploitable crash. *This bug could only be triggered when accessibility was enabled.*. This vulnerability affects Thunderbird < 78.12, Firefox ESR < 78.12, and Firefox < 90. **CVE ID : CVE-2021-29970**	https://www.mozilla.org/security/advisories/mfsa2021-30/, https://www.mozilla.org/security/advisories/mfsa2021-29/, https://www.mozilla.org/security/advisories/mfsa2021-28/	A-MOZ-THUN-180821/367
Out-of-bounds Write	05-Aug-21	6.8	Mozilla developers reported memory safety bugs present in code shared between Firefox and Thunderbird. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been	https://www.mozilla.org/security/advisories/mfsa2021-30/, https://www.mozilla.org/security/advisories/mfsa2	A-MOZ-THUN-180821/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.12, Firefox ESR < 78.12, and Firefox < 90. **CVE ID : CVE-2021-29976**	021-29/, https://www.mozilla.org/security/advisories/mfsa2021-28/	
naviwebs					
navigate_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-21	3.5	Cross Site Scripting (XSS) vulnerability in Naviwebs Navigate Cms 2.9 via the navigate-quickse parameter to 1) backups\backups.php, 2) blocks\blocks.php, 3) brands\brands.php, 4) comments\comments.php, 5) coupons\coupons.php, 6) feeds\feeds.php, 7) functions\functions.php, 8) items\items.php, 9) menus\menus.php, 10) orders\orders.php, 11) payment_methods\payment_methods.php, 12) products\products.php, 13) profiles\profiles.php, 14) shipping_methods\shipping_methods.php, 15) templates\templates.php, 16) users\users.php, 17) webdictionary\webdictionary.php, 18) websites\websites.php, and 19) webusers\webusers.php because the initial_url function is built in these files. **CVE ID : CVE-2021-36454**	https://github.com/NavigateCMS/Navigate-CMS/issues/24, https://www.navigatecms.com/en/blog/development/navigate_cms_update_2_9_4	A-NAV-NAVI-180821/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-21	6.5	SQL Injection vulnerability in Naviwebs Navigate CMS 2.9 via the quicksearch parameter in \lib\packages\comments\comments.php. **CVE ID : CVE-2021-36455**	https://www.navigatecms.com/en/blog/development/navigate_cms_update_2_9_4	A-NAV-NAVI-180821/370
Neo4j					
neo4j					
Deserialization of Untrusted Data	05-Aug-21	7.5	Neo4j through 3.4.18 (with the shell server enabled) exposes an RMI service that arbitrarily deserializes Java objects, e.g., through setSessionVariable. An attacker can abuse this for remote code execution because there are dependencies with exploitable gadget chains. **CVE ID : CVE-2021-34371**	N/A	A-NEO-NEO4-180821/371
Netapp					
cloud_manager					
Exposure of Sensitive Information to an Unauthorized Actor	06-Aug-21	4	NetApp Cloud Manager versions prior to 3.9.9 log sensitive information that is available only to authenticated users. Customers with auto-upgrade enabled should already be on a fixed version while customers using on-prem connectors with auto-upgrade disabled are advised to upgrade to a fixed version.	https://security.netapp.com/advisory/NTAP-20210805-0011	A-NET-CLOU-180821/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-26998		
Exposure of Sensitive Information to an Unauthorized Actor	06-Aug-21	4	NetApp Cloud Manager versions prior to 3.9.9 log sensitive information when an Active Directory connection fails. The logged information is available only to authenticated users. Customers with auto-upgrade enabled should already be on a fixed version while customers using on-prem connectors with auto-upgrade disabled are advised to upgrade to a fixed version. **CVE ID : CVE-2021-26999**	https://security.netapp.com/advisory/NTAP-20210805-0012	A-NET-CLOU-180821/373
nettle_project					
nettle					
Improper Input Validation	05-Aug-21	5	A flaw was found in the way nettle's RSA decryption functions handled specially crafted ciphertext. An attacker could use this flaw to provide a manipulated ciphertext leading to application crash and denial of service. **CVE ID : CVE-2021-3580**	https://bugzilla.redhat.com/show_bug.cgi?id=1967983	A-NET-NETT-180821/374
obsdian					
obsidian					
N/A	07-Aug-21	7.5	Obsidian before 0.12.12 does not require user confirmation for non-http/https URLs. **CVE ID : CVE-2021-38148**	https://forum.obsidian.md/t/obsidian-release-v0-12-12/21564	A-OBS-OBSI-180821/375
onair2_project					
onair2					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	02-Aug-21	7.5	The OnAir2 WordPress theme before 3.9.9.2 and QT KenthaRadio WordPress plugin before 2.0.2 have exposed proxy functionality to unauthenticated users, sending requests to this proxy functionality will have the web server fetch and display the content from any URI, this would allow for SSRF (Server Side Request Forgery) and RFI (Remote File Inclusion) vulnerabilities on the website. **CVE ID : CVE-2021-24472**	N/A	A-ONA-ONAI-180821/376
onenav_project					
onenav					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-21	3.5	OneNav beta 0.9.12 allows XSS via the Add Link feature. NOTE: the vendor's position is that there intentionally is not any XSS protection at present, because the attack risk is largely limited to a compromised account; however, XSS protection is planned for a future release. **CVE ID : CVE-2021-38138**	N/A	A-ONE-ONEN-180821/377
online_covid_vaccination_scheduler_system_project					
online_covid_vaccination_scheduler_system					
Unrestricted Upload of File with Dangerous Type	03-Aug-21	7.5	Sourcecodester Online Covid Vaccination Scheduler System 1.0 is affected vulnerable to Arbitrary File Upload. The admin panel has an upload function of profile photo accessible at	N/A	A-ONL-ONLI-180821/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			http://localhost/scheduler/admin/?page=user. An attacker could upload a malicious file such as shell.php with the Content-Type: image/png. Then, the attacker have to visit the uploaded profile photo to access the shell. **CVE ID : CVE-2021-36622**		
openplcproject					
openplc					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	OpenPLC runtime V3 through 2016-03-14 allows stored XSS via the Device Name to the web server's Add New Device page. **CVE ID : CVE-2021-3351**	N/A	A-OPE-OPEN-180821/379
Opentext					
brava\\!_desktop					
Access of Uninitialized Pointer	03-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.3.84 (package 16.6.3.134). 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 parsing of IGS files. The issue results from the lack of proper initialization of a pointer prior to accessing it.	N/A	A-OPE-BRAV-180821/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12690. **CVE ID : CVE-2021-31503**		
Untrusted Pointer Dereference	03-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.3.84 (package 16.6.3.134). 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 parsing of PDF files. The issue results from the lack of proper validation of a user-supplied value prior to dereferencing it as a pointer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12691. **CVE ID : CVE-2021-31504**	N/A	A-OPE-BRAV-180821/381
openwebif_project					
openwebif					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	3.5	In addBouquet in js/bqe.js in OpenWebif (aka e2openplugin-OpenWebif) through 1.4.7, inserting JavaScript into the Add Bouquet feature of the Bouquet Editor (i.e., bouqueteditor/api/addbouquet?name=) leads to Stored	https://github.com/E2OpenPlugins/e2openplugin-OpenWebif/issues/1387	A-OPE-OPEN-180821/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XSS. **CVE ID : CVE-2021-38113**		
openwrt					
openwrt					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	4.3	There is missing input validation of host names displayed in OpenWrt before 19.07.8. The Connection Status page of the luci web-interface allows XSS, which can be used to gain full control over the affected system via ICMP. **CVE ID : CVE-2021-32019**	N/A	A-OPE-OPEN-180821/383
optimocha					
speed_booster_pack					
Improper Control of Generation of Code ('Code Injection')	02-Aug-21	6.5	The Speed Booster Pack âš¡ PageSpeed Optimization Suite WordPress plugin before 4.2.0 did not validate its caching_exclude_urls and caching_include_query_strings settings before outputting them in a PHP file, which could lead to RCE **CVE ID : CVE-2021-24430**	N/A	A-OPT-SPEE-180821/384
pengutronix					
barebox					
N/A	02-Aug-21	5	crypto/digest.c in Pengutronix barebox through 2021.07.0 leaks timing information because memcmp is used during digest verification. **CVE ID : CVE-2021-37847**	https://github.com/saschahauer/barebox/commit/0a9f9a7410681e55362f8311537ebc7be	A-PEN-BARE-180821/385

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
				9ad0fbe	
N/A	02-Aug-21	5	common/password.c in Pengutronix barebox through 2021.07.0 leaks timing information because strncmp is used during hash comparison. **CVE ID : CVE-2021-37848**	https://github.com/sascha hauer/barebox/commit/a3337563c705bc8e0cf32f910b3e9e3c43d962ff	A-PEN-BARE-180821/386
phone_shop_sales_managements_system_project					
phone_shop_sales_managements_system					
Unrestricted Upload of File with Dangerous Type	03-Aug-21	7.5	Arbitrary File Upload in Sourcecodester Phone Shop Sales Management System 1.0 enables RCE. **CVE ID : CVE-2021-36623**	N/A	A-PHO-PHON-180821/387
pi-hole					
pi-hole					
Improper Control of Generation of Code ('Code Injection')	04-Aug-21	6.5	Pi-hole's Web interface provides a central location to manage a Pi-hole instance and review performance statistics. Prior to Pi-hole Web interface version 5.5.1, the `validDomainWildcard` preg_match filter allows a malicious character through that can be used to execute code, list directories, and overwrite sensitive files. The issue lies in the fact that one of the periods is not escaped, allowing any character to be used in its place. A patch for this vulnerability was released in version 5.5.1.	https://github.com/pi-hole/AdminLTE/security/advisories/GHSA-5cm9-6p3m-v259	A-PI--PI-H-180821/388

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-2021-32706		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-21	3.5	Pi-hole's Web interface provides a central location to manage a Pi-hole instance and review performance statistics. Prior to Pi-hole Web interface version 5.5.1, the function to add domains to blocklists or allowlists is vulnerable to a stored cross-site-scripting vulnerability. User input added as a wildcard domain to a blocklist or allowlist is unfiltered in the web interface. Since the payload is stored permanently as a wildcard domain, this is a persistent XSS vulnerability. A remote attacker can therefore attack administrative user accounts through client-side attacks. Pi-hole Web Interface version 5.5.1 contains a patch for this vulnerability. **CVE ID : CVE-2021-32793**	https://github.com/pi-hole/AdminLTE/security/advisories/GHSA-g3w6-q4fg-p8x8	A-PI--PI-H-180821/389
pickplugins					
post_grid					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	4.3	The slider import search feature and tab parameter of the Post Grid WordPress plugin before 2.1.8 settings are not properly sanitised before being output back in the pages, leading to Reflected Cross-Site Scripting issues **CVE ID : CVE-2021-24488**	N/A	A-PIC-POST-180821/390
Pimcore					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
adminbundle					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-21	5	Pimcore AdminBundle version 6.8.0 and earlier suffers from a SQL injection issue in the specificID variable used by the application. This issue was fixed in version 6.9.4 of the product. **CVE ID : CVE-2021-31869**	N/A	A-PIM-ADMI-180821/391
customer_management_framework					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-21	5	Pimcore Customer Data Framework version 3.0.0 and earlier suffers from a Boolean-based blind SQL injection issue in the $id parameter of the SegmentAssignmentController.php component of the application. This issue was fixed in version 3.0.2 of the product. **CVE ID : CVE-2021-31867**	N/A	A-PIM-CUST-180821/392
planview					
spigit					
N/A	05-Aug-21	5	The REST API in Planview Spigit 4.5.3 allows remote unauthenticated attackers to query sensitive user accounts data, as demonstrated by an api/v1/users/1 request. **CVE ID : CVE-2021-38095**	https://www.planview.com/products-solutions/products/spigit/	A-PLA-SPIG-180821/393
Plone					
isurlinportal					
URL Redirection	02-Aug-21	5.8	Products.isurlinportal is a replacement for	https://github.com/plone	A-PLO-ISUR-180821/394

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 Untrusted Site ('Open Redirect')			isURLInPortal method in Plone. Versions of Products.isurlinportal prior to 1.2.0 have an Open Redirect vulnerability. Various parts of Plone use the 'is url in portal' check for security, mostly to see if it is safe to redirect to a url. A url like `https://example.org` is not in the portal. The url `https:example.org` without slashes is considered to be in the portal. When redirecting, some browsers go to `https://example.org`, others give an error. Attackers may use this to redirect victims to their site, especially as part of a phishing attack. The problem has been patched in Products.isurlinportal 1.2.0. **CVE ID : CVE-2021-32806**	/Products.isurlinportal/commit/d4fd34990d18adf05a10dc5e2bb4b066798280ba, https://github.com/plone/Products.isurlinportal/security/advisories/GHSA-q3m9-9fj2-mfwr	
post_index_project					
post_index					
Cross-Site Request Forgery (CSRF)	02-Aug-21	6.8	The Post Index WordPress plugin is vulnerable to Cross-Site Request Forgery via the OptionsPage function found in the ~/php/settings.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 0.7.5. **CVE ID : CVE-2021-34637**	N/A	A-POS-POST-180821/395
premio					
mystickymenu					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The Floating Notification Bar, Sticky Menu on Scroll, and Sticky Header for Any Theme â€“ myStickymenu WordPress plugin before 2.5.2 does not sanitise or escape its Bar Text settings, allowing hight privilege users to use malicious JavaScript in it, leading to a Stored Cross-Site Scripting issue, which will be triggered in the plugin's setting, as well as all front-page of the blog (when the Welcome bar is active) **CVE ID : CVE-2021-24425**	N/A	A-PRE-MYST-180821/396
profilepress					
profilepress					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The User Registration, User Profiles, Login & Membership â€“ ProfilePress (Formerly WP User Avatar) WordPress plugin before 3.1.8 did not sanitise or escape some of its settings before saving them and outputting them back in the page, allowing high privilege users such as admin to set JavaScript payloads in them even when the unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24450**	N/A	A-PRO-PROF-180821/397
Progress					
moveit_transfer					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-21	7.5	In certain Progress MOVEit Transfer versions before 2021.0.4 (aka 13.0.4), SQL injection in the MOVEit Transfer web application could allow an unauthenticated remote attacker to gain access to the 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, or execute SQL statements that alter or delete database elements, via crafted strings sent to unique MOVEit Transfer transaction types. The fixed versions are 2019.0.8 (11.0.8), 2019.1.7 (11.1.7), 2019.2.4 (11.2.4), 2020.0.7 (12.0.7), 2020.1.6 (12.1.6), and 2021.0.4 (13.0.4). **CVE ID : CVE-2021-38159**	https://community.progress.com/s/article/MOVEit-Transfer-Vulnerability-August-6-2021, https://www.progress.com/moveit	A-PRO-MOVE-180821/398
Qemu					
qemu					
Release of Invalid Pointer or Reference	05-Aug-21	6.5	A flaw was found in the USB redirector device emulation of QEMU in versions prior to 6.1.0-rc2. It occurs when dropping packets during a bulk transfer from a SPICE client due to the packet queue being full. A malicious SPICE client could use this flaw to	https://bugzilla.redhat.com/show_bug.cgi?id=1989651	A-QEM-QEMU-180821/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			make QEMU call free() with faked heap chunk metadata, resulting in a crash of QEMU or potential code execution with the privileges of the QEMU process on the host. **CVE ID : CVE-2021-3682**		
Radare					
radare2					
Improper Input Validation	02-Aug-21	5	A vulnerability was found in Radare2 in version 5.3.1. Improper input validation when reading a crafted LE binary can lead to resource exhaustion and DoS. **CVE ID : CVE-2021-3673**	https://bugzilla.redhat.com/show_bug.cgi?id=1989130	A-RAD-RADA-180821/400
Redhat					
build_of_quarkus					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-BUIL-180821/401
codeready_studio					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-CODE-180821/402

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
			confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**		
data_grid					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-DATA-180821/403
descision_manager					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-DESC-180821/404
integration_camel_k					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing	https://bugzilla.redhat.com/show_bug.	A-RED-INTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**	cgi?id=1981407	180821/405
integration_camel_quarkus					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-INTE-180821/406
jboss_enterprise_application_platform					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-JBOS-180821/407
jboss_enterprise_application_platform_expansion_pack					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-JBOS-180821/408
jboss_fuse					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-JBOS-180821/409
openshift_application_runtimes					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final.	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-OPEN-180821/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-3642		
process_automation					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-PROC-180821/411
wildfly_elytron					
Observable Discrepancy	05-Aug-21	3.5	A flaw was found in Wildfly Elytron where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality. This flaw affectes Wildfly Elytron versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final. **CVE ID : CVE-2021-3642**	https://bugzilla.redhat.com/show_bug.cgi?id=1981407	A-RED-WILD-180821/412
Redmine					
redmine					
Insufficient Session Expiration	05-Aug-21	5	Redmine 4.2.0 and 4.2.1 allow existing user sessions to continue upon enabling two-factor authentication for the user's account, but the intended behavior is for those sessions to be terminated.	https://www.redmine.org/projects/redmine/wiki/Security_Advisories, https://www.redmine.org	A-RED-REDM-180821/413

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-2021-37156	/news/132	
robotbtc_project					
robotbtc					
Incorrect Authorization	03-Aug-21	5	A security flaw in the 'owned' function of a smart contract implementation for RobotCoin (RBTC), a tradeable Ethereum ERC20 token, allows attackers to hijack victim accounts and arbitrarily increase the digital supply of assets. **CVE ID : CVE-2021-34272**	N/A	A-ROB-ROBO-180821/414
roxy-wi					
roxy-wi					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-21	7.5	Roxy-WI through 5.2.2.0 allows SQL Injection via check_login. An unauthenticated attacker can extract a valid uuid to bypass authentication. **CVE ID : CVE-2021-38167**	N/A	A-ROX-ROXY-180821/415
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Aug-21	6.5	Roxy-WI through 5.2.2.0 allows authenticated SQL injection via select_servers. **CVE ID : CVE-2021-38168**	N/A	A-ROX-ROXY-180821/416
Improper Neutralization of Special Elements	07-Aug-21	6.5	Roxy-WI through 5.2.2.0 allows command injection via /app/funct.py and	N/A	A-ROX-ROXY-180821/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			/api/api_funct.py. **CVE ID : CVE-2021-38169**		
rsvpmaker_project					
rsvpmaker					
Server-Side Request Forgery (SSRF)	02-Aug-21	4	The Import feature of the RSVPMaker WordPress plugin before 8.7.3 (/wp-admin/tools.php?page=rsvpmaker_export_screen) takes an URL input and calls curl on it, without first validating it to ensure it's a remote one. As a result, a high privilege user could use that feature to scan the internal network via a SSRF attack. **CVE ID : CVE-2021-24371**	https://codevigilant.com/disclosure/2021/wp-plugin-rsvpmaker/	A-RSV-RSVP-180821/418
Ruby-lang					
Ruby					
Inadequate Encryption Strength	01-Aug-21	5.8	An issue was discovered in Ruby through 2.6.7, 2.7.x through 2.7.3, and 3.x through 3.0.1. Net::IMAP does not raise an exception when StartTLS fails with an an unknown response, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack." **CVE ID : CVE-2021-32066**	https://github.com/ruby/ruby/commit/a21a3b7d23704a01d34bd79d09dc37897e00922a, https://www.ruby-lang.org/en/news/2021/07/07/starttls-stripping-in-net-imap/, https://hack	A-RUB-RUBY-180821/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				erone.com/reports/1178562	
salesforce					
mule					
Improper Restriction of XML External Entity Reference	05-Aug-21	5	XML external entity (XXE) vulnerability affecting certain versions of a Mule runtime component that may affect CloudHub, GovCloud, Runtime Fabric, Pivotal Cloud Foundry, Private Cloud Edition, and on-premise customers. **CVE ID : CVE-2021-1630**	https://help.salesforce.com/articleView?id=000362693&type=1&mode=1	A-SAL-MULE-180821/420
Samsung					
internet					
Improper Authentication	05-Aug-21	5	Unprotected component vulnerability in Samsung Internet prior to version 14.2 allows untrusted application to access internal files in Samsung Internet. **CVE ID : CVE-2021-25445**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=8	A-SAM-INTE-180821/421
smart_touch_call					
Improper Authentication	05-Aug-21	5	Improper access control vulnerability in Smart Touch Call prior to version 1.0.0.5 allows arbitrary webpage loading in webview. **CVE ID : CVE-2021-25448**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=8	A-SAM-SMAR-180821/422
Seeddms					
seeddms					
Cross-Site Request Forgery	03-Aug-21	4.3	Cross-Site Request Forgery (CSRF) vulnerability in the /op/op.Ajax.php in SeedDMS	N/A	A-SEE-SEED-180821/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			v5.1.x<5.1.23 and v6.0.x<6.0.16 allows a remote attacker to edit document name without victim's knowledge, by enticing an authenticated user to visit an attacker's web page. **CVE ID : CVE-2021-35343**		
Cross-Site Request Forgery (CSRF)	03-Aug-21	4.3	Cross-Site Request Forgery (CSRF) vulnerability in the /op/op.LockDocument.php in SeedDMS v5.1.x<5.1.23 and v6.0.x <6.0.16 allows a remote attacker to lock any document without victim's knowledge, by enticing an authenticated user to visit an attacker's web page. **CVE ID : CVE-2021-36542**	N/A	A-SEE-SEED-180821/424
Cross-Site Request Forgery (CSRF)	03-Aug-21	4.3	Cross-Site Request Forgery (CSRF) vulnerability in the /op/op.UnlockDocument.php in SeedDMS v5.1.x <5.1.23 and v6.0.x <6.0.16 allows a remote attacker to unlock any document without victim's knowledge, by enticing an authenticated user to visit an attacker's web page. **CVE ID : CVE-2021-36543**	N/A	A-SEE-SEED-180821/425
seo_backlinks_project					
seo_backlinks					
Cross-Site Request Forgery (CSRF)	02-Aug-21	6.8	The SEO Backlinks WordPress plugin is vulnerable to Cross-Site Request Forgery via the loc_config function found in the ~/seo-backlinks.php file	N/A	A-SEO-SEO_-180821/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which allows attackers to inject arbitrary web scripts, in versions up to and including 4.0.1. **CVE ID : CVE-2021-34632**		
showdoc					
showdoc					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	04-Aug-21	4.3	showdoc is vulnerable to Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) **CVE ID : CVE-2021-3678**	https://github.com/star7th/showdoc/commit/4b962c1740311e0d46775023b6acba39ad60e370, https://huntr.dev/bounties/f9a9defd-29ea-4442-b692-ff1512813de4	A-SHO-SHOW-180821/427
Inadequate Encryption Strength	04-Aug-21	4	showdoc is vulnerable to Missing Cryptographic Step **CVE ID : CVE-2021-3680**	https://huntr.dev/bounties/76b49607-fba9-4100-9be7-cb459fe6cfe2 , https://github.com/star7th/showdoc/commit/4b962c1740311e0d46775023b6acba39ad60e370	A-SHO-SHOW-180821/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
skytable					
skytable					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-21	9.4	Skytable is a NoSQL database with automated snapshots and TLS. Versions prior to 0.5.1 are vulnerable to a a directory traversal attack enabling remotely connected clients to destroy and/or manipulate critical files on the host's file system. This security bug has been patched in version 0.5.1. There are no known workarounds aside from upgrading. **CVE ID : CVE-2021-32814**	https://github.com/skytable/skytable/security/advisories/GHSA-2hj9-cxmc-m4g7, https://security.skytable.io/ve/s/00001.html	A-SKY-SKYT-180821/429
Unchecked Return Value	05-Aug-21	5	Skytable is an open source NoSQL database. In versions prior to 0.6.4 an incorrect check of return value of the accept function in the run-loop for a TCP socket/TLS socket/TCP+TLS multi-socket causes an early exit from the run loop that should continue infinitely unless terminated by a local user, effectively causing the whole database server to shut down. This has severe impact and can be used to easily cause DoS attacks without the need to use much bandwidth. The attack vectors include using an incomplete TLS connection for example by not providing the certificate for the connection and using a	https://github.com/skytable/skytable/commit/bb19d024ea1e5e0c9a3d75a9ee58ff03c70c7e5d, https://github.com/skytable/skytable/security/advisories/GHSA-q27r-h25m-hcc7, https://security.skytable.io/ve/s/00002.html	A-SKY-SKYT-180821/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted TCP packet that triggers the application layer backoff algorithm. **CVE ID : CVE-2021-37625**		
sola-newsletters_project					
sola-newsletters					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	The Nifty Newsletters WordPress plugin is vulnerable to Cross-Site Request Forgery via the sola_nl_wp_head function found in the ~/sola-newsletters.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 4.0.23. **CVE ID : CVE-2021-34634**	N/A	A-SOL-SOLA-180821/431
sourcegraph					
sourcegraph					
N/A	02-Aug-21	4	Sourcegraph is a code search and navigation engine. Sourcegraph before version 3.30.0 has two potential information leaks. The site-admin area can be accessed by regular users and all information and features are properly protected except for daily usage statistics and code intelligence uploads and indexes. It is not possible to alter the information, nor interact with any other features in the site-admin area. The issue is patched in version 3.30.0, where the	https://github.com/sourcegraph/sourcegraph/security/advisories/GHSA-mq5p-477h-xgwv, https://github.com/sourcegraph/sourcegraph/commit/6e51f4546368d959a1f9f173d16e5f20c55deb56	A-SOU-SOUR-180821/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information cannot be accessed by unprivileged users. There are no workarounds aside from upgrading. **CVE ID : CVE-2021-32787**		
southsoft					
graduate_management_information_system					
Cross-Site Request Forgery (CSRF)	06-Aug-21	6.8	Southsoft GMIS 5.0 is vulnerable to CSRF attacks. Attackers can access other users' private information such as photos through CSRF. For example: any student's photo information can be accessed through /gmis/(S([1]))/student/grgl/PotoImageShow/?bh=[2]. Among them, the code in [1] is a random string generated according to the user's login related information. It can protect the user's identity, but it can not effectively prevent unauthorized access. The code in [2] is the student number of any student. The attacker can carry out CSRF attack on the system by modifying [2] without modifying [1]. **CVE ID : CVE-2021-37381**	N/A	A-SOU-GRAD-180821/433
steam_group_viewer_project					
steam_group_viewer					
Improper Neutralization of Input	02-Aug-21	3.5	The Steam Group Viewer WordPress plugin through 2.1 does not sanitise or escape its	N/A	A-STE-STEA-180821/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			"Steam Group Address" settings before outputting it in the page, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24476**		
tar_project					
tar					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-21	5.8	The npm package "tar" (aka node-tar) before versions 6.1.2, 5.0.7, 4.4.15, and 3.2.3 has an arbitrary File Creation/Overwrite vulnerability via insufficient symlink protection. \`node-tar\` aims to guarantee that any file whose location would be modified by a symbolic link is not extracted. This is, in part, achieved by ensuring that extracted directories are not symlinks. Additionally, in order to prevent unnecessary \`stat\` calls to determine whether a given path is a directory, paths are cached when directories are created. This logic was insufficient when extracting tar files that contained both a directory and a symlink with the same name as the directory. This order of operations resulted in the directory being created and added to the \`node-tar\` directory cache. When a directory is present in the directory cache, subsequent	https://github.com/npm/node-tar/security/advisories/GHSA-r628-mhmh-qjhw, https://github.com/npm/node-tar/commit/9dbdeb6df8e9dbd96fa9e84341b9d74734be6c20	A-TAR-TAR-180821/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			calls to mkdir for that directory are skipped. However, this is also where `node-tar` checks for symlinks occur. By first creating a directory, and then replacing that directory with a symlink, it was thus possible to bypass `node-tar` symlink checks on directories, essentially allowing an untrusted tar file to symlink into an arbitrary location and subsequently extracting arbitrary files into that location, thus allowing arbitrary file creation and overwrite. This issue was addressed in releases 3.2.3, 4.4.15, 5.0.7 and 6.1.2. **CVE ID : CVE-2021-32803**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-21	5.8	The npm package "tar" (aka node-tar) before versions 6.1.1, 5.0.6, 4.4.14, and 3.3.2 has a arbitrary File Creation/Overwrite vulnerability due to insufficient absolute path sanitization. node-tar aims to prevent extraction of absolute file paths by turning absolute paths into relative paths when the `preservePaths` flag is not set to `true`. This is achieved by stripping the absolute path root from any absolute file paths contained in a tar file. For example `/home/user/.bashrc` would turn into	https://github.com/npm/node-tar/commit/1f036ca23f64a547bdd6c79c1a44bc62e8115da4, https://github.com/npm/node-tar/security/advisories/GHSA-3jfq-g458-7qm9	A-TAR-TAR-180821/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`home/user/.bashrc`. This logic was insufficient when file paths contained repeated path roots such as `////home/user/.bashrc`. `node-tar` would only strip a single path root from such paths. When given an absolute file path with repeating path roots, the resulting path (e.g. `///home/user/.bashrc`) would still resolve to an absolute path, thus allowing arbitrary file creation and overwrite. This issue was addressed in releases 3.2.2, 4.4.14, 5.0.6 and 6.1.1. Users may work around this vulnerability without upgrading by creating a custom `onentry` method which sanitizes the `entry.path` or a `filter` method which removes entries with absolute paths. See referenced GitHub Advisory for details. Be aware of CVE-2021-32803 which fixes a similar bug in later versions of tar. **CVE ID : CVE-2021-32804**		
taxopress					
taxopress					
Improper Neutralization of Input During Web	02-Aug-21	3.5	The TaxoPress â€“ Create and Manage Taxonomies, Tags, Categories WordPress plugin before 3.7.0.2 does not	N/A	A-TAX-TAXO-180821/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			sanitise its Taxonomy description field, allowing high privilege users to set JavaScript payload in them even when the unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24444**		
Tecnick					
tcexam					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-21	4.3	A reflected cross-site scripting vulnerability exists in TCExam <= 14.8.3. The paths provided in the f, d, and dir parameters in tce_filemanager.php were not properly validated and could cause reflected XSS via the unsanitized output of the path supplied. An attacker could craft a malicious link which, if triggered by an administrator, could result in the attacker hijacking the victim's session or performing actions on their behalf. **CVE ID : CVE-2021-20115**	https://www.tenable.com/security/research/tra-2021-32	A-TEC-TCEX-180821/438
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-21	4.3	A reflected cross-site scripting vulnerability exists in TCExam <= 14.8.4. The paths provided in the f, d, and dir parameters in tce_select_mediafile.php were not properly validated and could cause reflected XSS via the unsanitized output of the path supplied. An attacker could craft a malicious link	N/A	A-TEC-TCEX-180821/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which, if triggered by an administrator, could result in the attacker hijacking the victim's session or performing actions on their behalf. **CVE ID : CVE-2021-20116**		
tekmonks					
monkshu					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	4.3	Monkshu is an enterprise application server for mobile apps (iOS and Android), responsive HTML 5 apps, and JSON API services. In version 2.90 and earlier, there is a reflected cross-site scripting vulnerability in frontend HTTP server. The attacker can send in a carefully crafted URL along with a known bug in the server which will cause a 500 error, and the response will then embed the URL provided by the hacker. The impact is moderate as the hacker must also be able to craft an HTTP request which should cause a 500 server error. None such requests are known as this point. The issue is patched in version 2.95. As a workaround, one may use a disk caching plugin. **CVE ID : CVE-2021-32812**	https://github.com/TekMonksGitHub/monkshu/security/advisories/GHSA-hcpx-66hq-7g4x, https://github.com/TekMonksGitHub/monkshu/commit/4601a9bfdc934d7ac32619ce621652fad0cf452b	A-TEK-MONK-180821/440
thememason					
popular_brand_icons_-_simple_icons					
Improper Neutralizatio	02-Aug-21	3.5	The Popular Brand Icons â€" Simple Icons WordPress	N/A	A-THE-POPU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			plugin before 2.7.8 does not sanitise or validate some of its shortcode parameters, such as "color", "size" or "class", allowing users with a role as low as Contributor to set Cross-Site payload in them. A post made by a contributor would still have to be approved by an admin to have the XSS triggered in the frontend, however, higher privilege users, such as editor could exploit this without the need of approval, and even when the blog disallows the unfiltered_html capability. **CVE ID : CVE-2021-24503**		180821/441
themeum					
tutor_lms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The Tutor LMS â€“ eLearning and online course solution WordPress plugin before 1.9.2 did not escape the Summary field of Announcements (when outputting it in an attribute), which can be created by users as low as Tutor Instructor. This lead to a Stored Cross-Site Scripting issue, which is triggered when viewing the Announcements list, and could result in privilege escalation when viewed by an admin. **CVE ID : CVE-2021-24455**	N/A	A-THE-TUTO-180821/442
traefik					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
traefik					
Improper Control of Dynamically-Managed Code Resources	03-Aug-21	6.8	Traefik is an HTTP reverse proxy and load balancer. Prior to version 2.4.13, there exists a potential header vulnerability in Traefik's handling of the Connection header. Active exploitation of this issue is unlikely, as it requires that a removed header would lead to a privilege escalation, however, the Traefik team has addressed this issue to prevent any potential abuse. If one has a chain of Traefik middlewares, and one of them sets a request header, then sending a request with a certain Connection header will cause it to be removed before the request is sent. In this case, the backend does not see the request header. A patch is available in version 2.4.13. There are no known workarounds aside from upgrading. **CVE ID : CVE-2021-32813**	https://github.com/traefik/traefik/pull/8319/commits/cbaf86a93014a969b8accf39301932c17d0d73f9, https://github.com/traefik/traefik/security/advisories/GHSA-m697-4v8f-55qg	A-TRA-TRAE-180821/443
Trendmicro					
apex_one					
Incorrect Default Permissions	04-Aug-21	7.2	An incorrect permission assignment privilege escalation vulnerability in Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security Services could allow an	https://success.trendmicro.com/jp/solution/000287796, https://success.trendmicr	A-TRE-APEX-180821/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to modify a specific script before it is executed. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-32464**	o.com/solution/000287819, https://success.trendmicro.com/solution/000286857	
Improper Preservation of Permissions	04-Aug-21	6.5	An incorrect permission preservation vulnerability in Trend Micro Apex One, Apex One as a Service and OfficeScan XG SP1 could allow a remote user to perform an attack and bypass authentication on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-32465**	https://success.trendmicro.com/jp/solution/000287796, https://success.trendmicro.com/solution/000287819	A-TRE-APEX-180821/445
officescan					
Incorrect Default Permissions	04-Aug-21	7.2	An incorrect permission assignment privilege escalation vulnerability in Trend Micro Apex One, Apex One as a Service and Worry-Free Business Security Services could allow an attacker to modify a specific script before it is executed. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	https://success.trendmicro.com/jp/solution/000287796, https://success.trendmicro.com/solution/000287819, https://success.trendmicro.com/solution/0002868	A-TRE-OFFI-180821/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-32464	57	
Improper Preservation of Permissions	04-Aug-21	6.5	An incorrect permission preservation vulnerability in Trend Micro Apex One, Apex One as a Service and OfficeScan XG SP1 could allow a remote user to perform an attack and bypass authentication on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2021-32465**	https://success.trendmicro.com/jp/solution/000287796, https://success.trendmicro.com/solution/000287819	A-TRE-OFFI-180821/447
unidocs					
ezpdfreader					
Improper Input Validation	05-Aug-21	7.5	An improper input validation vulnerability in the service of ezPDFReader allows attacker to execute arbitrary command. This issue occurred when the ezPDF launcher received and executed crafted input values through JSON-RPC communication. **CVE ID : CVE-2021-26605**	N/A	A-UNI-EZPD-180821/448
weblizar					
admin_custom_login					
Cross-Site Request Forgery (CSRF)	02-Aug-21	6.8	The Admin Custom Login WordPress plugin is vulnerable to Cross-Site Request Forgery due to the loginbgSave action found in the ~/includes/Login-form-setting/Login-form-	N/A	A-WEB-ADMI-180821/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			background.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 3.2.7. **CVE ID : CVE-2021-34628**		
wpdevart					
youtube_embed\\,_playlist_and_popup					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The YouTube Embed, Playlist and Popup by WpDevArt WordPress plugin before 2.3.9 did not escape, validate or sanitise some of its shortcode options, available to users with a role as low as Contributor, leading to an authenticated Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24464**	N/A	A-WPD-YOUT-180821/450
wpdownloadmanager					
wordpress_download_manager					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-21	4	Authenticated Directory Traversal in WordPress Download Manager <= 3.1.24 allows authenticated (Contributor+) users to obtain sensitive configuration file information, as well as allowing Author+ users to perform XSS attacks, by setting Download template to a file containing configuration information or an uploaded JavaScript with an image extension This issue affects: WordPress Download Manager version 3.1.24 and	N/A	A-WPD-WORD-180821/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior versions. **CVE ID : CVE-2021-34638**		
Unrestricted Upload of File with Dangerous Type	05-Aug-21	6.5	Authenticated File Upload in WordPress Download Manager <= 3.1.24 allows authenticated (Author+) users to upload files with a double extension, e.g. "payload.php.png" which is executable in some configurations. This issue affects: WordPress Download Manager version 3.1.24 and prior versions. **CVE ID : CVE-2021-34639**	N/A	A-WPD-WORD-180821/452
wplearnmanager					
wp_learn_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	4.3	The WP LMS â€“ Best WordPress LMS Plugin WordPress plugin through 1.1.2 does not properly sanitise or validate its User Field Titles, allowing XSS payload to be used in them. Furthermore, no CSRF and capability checks were in place, allowing such attack to be performed either via CSRF or as any user (including unauthenticated) **CVE ID : CVE-2021-24504**	N/A	A-WPL-WP_L-180821/453
yada_wiki_project					
yada_wiki					
Improper Neutralization of Input	02-Aug-21	3.5	The Yada Wiki WordPress plugin before 3.4.1 did not sanitise, validate or escape	N/A	A-YAD-YADA-180821/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			the anchor attribute of its shortcode, leading to a Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24470**		
Yandex					
yandex_turbo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	3.5	The RSS for Yandex Turbo WordPress plugin through 1.30 does not sanitise or escape some of its settings before saving and outputing them in the admin dashboard, leading to an Authenticated Stored Cross-Site Scripting issue even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24428**	N/A	A-YAN-YAND-180821/455
youtube_feeder_project					
youtube_feeder					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	The Youtube Feeder WordPress plugin is vulnerable to Cross-Site Request Forgery via the printAdminPage function found in the ~/youtube-feeder.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 2.0.1. **CVE ID : CVE-2021-34633**	N/A	A-YOU-YOUT-180821/456
ypsomed					
mylife					
N/A	02-Aug-21	4.3	Ypsomed mylife Cloud, mylife Mobile Application, Ypsomed	N/A	A-YPS-MYLI-180821/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mylife Cloud: All versions prior to 1.7.2, Ypsomed mylife App: All versions prior to 1.7.5,The application layer encryption of the communication protocol between the Ypsomed mylife App and mylife Cloud uses non-random IVs, which allows man-in-the-middle attackers to tamper with messages. **CVE ID : CVE-2021-27499**		
Use of Hard-coded Credentials	02-Aug-21	5.8	Ypsomed mylife Cloud, mylife Mobile Application, Ypsomed mylife Cloud: All versions prior to 1.7.2, Ypsomed mylife App: All versions prior to 1.7.5,The application encrypts on the application layer of the communication protocol between the Ypsomed mylife App and mylife Cloud credentials based on hard-coded secrets, which allows man-in-the-middle attackers to tamper with messages. **CVE ID : CVE-2021-27503**	N/A	A-YPS-MYLI-180821/458
mylife_cloud					
N/A	02-Aug-21	4.3	Ypsomed mylife Cloud, mylife Mobile Application, Ypsomed mylife Cloud: All versions prior to 1.7.2, Ypsomed mylife App: All versions prior to 1.7.5,The application layer encryption of the communication protocol between the Ypsomed mylife App and mylife Cloud uses	N/A	A-YPS-MYLI-180821/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			non-random IVs, which allows man-in-the-middle attackers to tamper with messages. **CVE ID : CVE-2021-27499**		
Use of Hard-coded Credentials	02-Aug-21	5.8	Ypsomed mylife Cloud, mylife Mobile Application, Ypsomed mylife Cloud: All versions prior to 1.7.2, Ypsomed mylife App: All versions prior to 1.7.5,The application encrypts on the application layer of the communication protocol between the Ypsomed mylife App and mylife Cloud credentials based on hard-coded secrets, which allows man-in-the-middle attackers to tamper with messages. **CVE ID : CVE-2021-27503**	N/A	A-YPS-MYLI-180821/460
Zope					
accesscontrol					
Improperly Controlled Modification of Dynamically-Determined Object Attributes	02-Aug-21	6.5	Zope is an open-source web application server. Zope versions prior to versions 4.6.3 and 5.3 have a remote code execution security issue. In order to be affected, one must use Python 3 for one's Zope deployment, run Zope 4 below version 4.6.3 or Zope 5 below version 5.3, and have the optional `Products.PythonScripts` add-on package installed. By default, one must have the admin-level Zope "Manager" role to add or edit Script (Python) objects through the	https://github.com/zopefoundation/Zope/security/advisories/GHSA-g4gq-j4p2-j8fr, https://github.com/zopefoundation/Zope/commit/f72a18dda8e9bf2aedb4616876166846 4a4be988	A-ZOP-ACCE-180821/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web. Only sites that allow untrusted users to add/edit these scripts through the web are at risk. Zope releases 4.6.3 and 5.3 are not vulnerable. As a workaround, a site administrator can restrict adding/editing Script (Python) objects through the web using the standard Zope user/role permission mechanisms. Untrusted users should not be assigned the Zope Manager role and adding/editing these scripts through the web should be restricted to trusted users only. This is the default configuration in Zope. **CVE ID : CVE-2021-32811**		
Zope					
Improperly Controlled Modification of Dynamically-Determined Object Attributes	02-Aug-21	6.5	Zope is an open-source web application server. Zope versions prior to versions 4.6.3 and 5.3 have a remote code execution security issue. In order to be affected, one must use Python 3 for one's Zope deployment, run Zope 4 below version 4.6.3 or Zope 5 below version 5.3, and have the optional `Products.PythonScripts` add-on package installed. By default, one must have the admin-level Zope "Manager" role to add or edit Script (Python) objects through the web. Only sites that allow	https://github.com/zopefoundation/Zope/security/advisories/GHSA-g4gq-j4p2-j8fr, https://github.com/zopefoundation/Zope/commit/f72a18dda8e9bf2aedb4616876166846 4a4be988	A-ZOP-ZOPE-180821/462

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
			untrusted users to add/edit these scripts through the web are at risk. Zope releases 4.6.3 and 5.3 are not vulnerable. As a workaround, a site administrator can restrict adding/editing Script (Python) objects through the web using the standard Zope user/role permission mechanisms. Untrusted users should not be assigned the Zope Manager role and adding/editing these scripts through the web should be restricted to trusted users only. This is the default configuration in Zope. **CVE ID : CVE-2021-32811**		
Hardware					
bosch					
aviotec					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	H-BOS-AVIO-180821/463
cpp13					
Cross-Site	05-Aug-21	6.8	A vulnerability in the web-	https://psirt.	H-BOS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	bosch.com/security-advisories/bosch-sa-033305-bt.html	CPP1-180821/464
cpp14					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	H-BOS-CPP1-180821/465
cpp4					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	H-BOS-CPP4-180821/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			logged in into the camera. **CVE ID : CVE-2021-23849**		
cpp6					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	H-BOS-CPP6-180821/467
cpp7					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	H-BOS-CPP7-180821/468
cpp7.3					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross	https://psirt.bosch.com/security-advisories/bosch-sa-033305-	H-BOS-CPP7-180821/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	bt.html	
Cisco					
small_business_rv160					
Improper Input Validation	04-Aug-21	10	A vulnerability in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges. Due to the nature of the vulnerability, only commands without parameters can be executed. **CVE ID : CVE-2021-1602**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4	H-CIS-SMAL-180821/470
small_business_rv160w					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-Aug-21	10	A vulnerability in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges. Due to the nature of the vulnerability, only commands without parameters can be executed. **CVE ID : CVE-2021-1602**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4	H-CIS-SMAL-180821/471
small_business_rv260					
Improper Input Validation	04-Aug-21	10	A vulnerability in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4	H-CIS-SMAL-180821/472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges. Due to the nature of the vulnerability, only commands without parameters can be executed. **CVE ID : CVE-2021-1602**		
small_business_rv260p					
Improper Input Validation	04-Aug-21	10	A vulnerability in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges. Due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4	H-CIS-SMAL-180821/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the nature of the vulnerability, only commands without parameters can be executed. **CVE ID : CVE-2021-1602**		
small_business_rv260w					
Improper Input Validation	04-Aug-21	10	A vulnerability in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges. Due to the nature of the vulnerability, only commands without parameters can be executed. **CVE ID : CVE-2021-1602**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4	H-CIS-SMAL-180821/474
small_business_rv340					
N/A	04-Aug-21	10	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W,	https://tools.cisco.com/security/center/content/Cis	H-CIS-SMAL-180821/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1609**	coSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy	
N/A	04-Aug-21	9	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1610**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy	H-CIS-SMAL-180821/476
small_business_rv340w					
N/A	04-Aug-21	10	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-	H-CIS-SMAL-180821/477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1609**	pY8J3qfy	
N/A	04-Aug-21	9	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1610**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy	H-CIS-SMAL-180821/478
small_business_rv345					
N/A	04-Aug-21	10	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy	H-CIS-SMAL-180821/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advisory. **CVE ID : CVE-2021-1609**		
N/A	04-Aug-21	9	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1610**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy	H-CIS-SMAL-180821/480
small_business_rv345p					
N/A	04-Aug-21	10	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1609**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy	H-CIS-SMAL-180821/481
N/A	04-Aug-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/se	H-CIS-SMAL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1610**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy	180821/482
Dlink					
dir-615					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Aug-21	7.5	A buffer overflow in D-Link DIR-615 C2 3.03WW. The ping_ipaddr parameter in ping_response.cgi POST request allows an attacker to crash the webserver and might even gain remote code execution. **CVE ID : CVE-2021-37388**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--180821/483
ecobee					
ecobee3_lite					
Use of Hard-coded Credentials	03-Aug-21	5	Hardcoded default root credentials exist on the ecobee3 lite 4.5.81.200 device. This allows a threat actor to gain access to the password-protected bootloader environment through the serial console. **CVE ID : CVE-2021-27952**	N/A	H-ECO-ECOB-180821/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Aug-21	7.8	A NULL pointer dereference vulnerability exists on the ecobee3 lite 4.5.81.200 device in the HomeKit Wireless Access Control setup process. A threat actor can exploit this vulnerability to cause a denial of service, forcing the device to reboot via a crafted HTTP request. **CVE ID : CVE-2021-27953**	N/A	H-ECO-ECOB-180821/485
Out-of-bounds Write	03-Aug-21	6.4	A heap-based buffer overflow vulnerability exists on the ecobee3 lite 4.5.81.200 device in the HKProcessConfig function of the HomeKit Wireless Access Control setup process. A threat actor can exploit this vulnerability to force the device to connect to a SSID or cause a denial of service. **CVE ID : CVE-2021-27954**	N/A	H-ECO-ECOB-180821/486
Huawei					
ecns280_td					
Improper Privilege Management	02-Aug-21	4.6	There is a privilege escalation vulnerability in some Huawei products. Due to improper privilege management, a local attacker with common privilege may access some specific files in the affected products. Successful exploit will cause privilege escalation.Affected product versions include:eCNS280_TD V100R005C00,V100R005C10; eSE620X vESS	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-privilege-en	H-HUA-ECNS-180821/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V100R001C10SPC200,V100R001C20SPC200. **CVE ID : CVE-2021-22396**		
ese620x_vess					
Improper Privilege Management	02-Aug-21	4.6	There is a privilege escalation vulnerability in some Huawei products. Due to improper privilege management, a local attacker with common privilege may access some specific files in the affected products. Successful exploit will cause privilege escalation.Affected product versions include:eCNS280_TD V100R005C00,V100R005C10;eSE620X vESS V100R001C10SPC200,V100R001C20SPC200. **CVE ID : CVE-2021-22396**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-privilege-en	H-HUA-ESE6-180821/488
hulk-al00c					
Incorrect Authorization	02-Aug-21	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations. Affected product versions include: Hulk-AL00C 9.1.1.201(C00E201R8P1);Jennifer-AN00C 10.1.1.171(C00E170R6P3);Jenny-AL10B 10.1.0.228(C00E220R5P1)	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-smartphone-en	H-HUA-HULK-180821/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and OxfordPL-AN10B 10.1.0.116(C00E110R2P1). **CVE ID : CVE-2021-22398**		
jennifer-an00c					
Incorrect Authorization	02-Aug-21	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations. Affected product versions include: Hulk-AL00C 9.1.1.201(C00E201R8P1);Jennifer-AN00C 10.1.1.171(C00E170R6P3);Jenny-AL10B 10.1.0.228(C00E220R5P1) and OxfordPL-AN10B 10.1.0.116(C00E110R2P1). **CVE ID : CVE-2021-22398**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-smartphone-en	H-HUA-JENN-180821/490
jenny-al10b					
Incorrect Authorization	02-Aug-21	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations. Affected product versions include: Hulk-AL00C 9.1.1.201(C00E201R8P1);Jen	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-smartphone-en	H-HUA-JENN-180821/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			nifer-AN00C 10.1.1.171(C00E170R6P3);Jenny-AL10B 10.1.0.228(C00E220R5P1) and OxfordPL-AN10B 10.1.0.116(C00E110R2P1). **CVE ID : CVE-2021-22398**		
oxfordpl-an10b					
Incorrect Authorization	02-Aug-21	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations. Affected product versions include: Hulk-AL00C 9.1.1.201(C00E201R8P1);Jennifer-AN00C 10.1.1.171(C00E170R6P3);Jenny-AL10B 10.1.0.228(C00E220R5P1) and OxfordPL-AN10B 10.1.0.116(C00E110R2P1). **CVE ID : CVE-2021-22398**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-smartphone-en	H-HUA-OXFO-180821/492
oxfords-an00a					
Improper Input Validation	03-Aug-21	4.3	Some Huawei Smartphones has an insufficient input validation vulnerability due to the lack of parameter validation. An attacker may trick a user into installing a malicious APP. The app can modify specific parameters, causing the system to crash.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210721-01-phones-	H-HUA-OXFO-180821/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Affected product include:OxfordS-AN00A 10.0.1.10(C00E10R1P1),10.0.1.105(C00E103R3P3),10.0.1.115(C00E110R3P3),10.0.1.123(C00E121R3P3),10.0.1.135(C00E130R3P3),10.0.1.135(C00E130R4P1),10.0.1.152(C00E140R4P1),10.0.1.160(C00E160R4P1),10.0.1.167(C00E166R4P1),10.0.1.173(C00E172R5P1),10.0.1.178(C00E175R5P1) and 10.1.0.202(C00E79R5P1). **CVE ID : CVE-2021-22400**	en	
openplcproject					
openplc_v3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Aug-21	9	Command Injection in Open PLC Webserver v3 allows remote attackers to execute arbitrary code via the "Hardware Layer Code Box" component on the "/hardware" page of the application. **CVE ID : CVE-2021-31630**	N/A	H-OPE-OPEN-180821/494
prolink					
prc2402m					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Aug-21	7.5	In ProLink PRC2402M V1.0.18 and older, the set_TR069 function in the adm.cgi binary, accessible with a page parameter value of TR069 contains a trivial command injection where the value of the TR069_local_port parameter is passed directly to system.	N/A	H-PRO-PRC2-180821/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36705		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Aug-21	7.5	In ProLink PRC2402M V1.0.18 and older, the set_sys_cmd function in the adm.cgi binary, accessible with a page parameter value of sysCMD contains a trivial command injection where the value of the command parameter is passed directly to system. **CVE ID : CVE-2021-36706**	N/A	H-PRO-PRC2-180821/496
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Aug-21	7.5	In ProLink PRC2402M V1.0.18 and older, the set_ledonoff function in the adm.cgi binary, accessible with a page parameter value of ledonoff contains a trivial command injection where the value of the led_cmd parameter is passed directly to do_system. **CVE ID : CVE-2021-36707**	N/A	H-PRO-PRC2-180821/497
Weak Password Recovery Mechanism for Forgotten Password	06-Aug-21	5	In ProLink PRC2402M V1.0.18 and older, the set_sys_init function in the login.cgi binary allows an attacker to reset the password to the administrative interface of the router. **CVE ID : CVE-2021-36708**	N/A	H-PRO-PRC2-180821/498
qsan					
xn8008t					
Improper Neutralization of Input During Web Page Generation	02-Aug-21	4.3	QSAN Storage Manager header page parameters does not filter special characters. Remote attackers can inject JavaScript without logging in and launch reflected XSS	N/A	H-QSA-XN80-180821/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacks to access and modify specific data. **CVE ID : CVE-2021-37216**		
xn8024r					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	4.3	QSAN Storage Manager header page parameters does not filter special characters. Remote attackers can inject JavaScript without logging in and launch reflected XSS attacks to access and modify specific data. **CVE ID : CVE-2021-37216**	N/A	H-QSA-XN80-180821/500
Samsung					
smartthings					
Improper Authentication	05-Aug-21	5	Improper access control vulnerability in SmartThings prior to version 1.7.67.25 allows untrusted applications to cause arbitrary webpage loading in webview. **CVE ID : CVE-2021-25446**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=8	H-SAM-SMAR-180821/501
Improper Authentication	05-Aug-21	5	Improper access control vulnerability in SmartThings prior to version 1.7.67.25 allows untrusted applications to cause local file inclusion in webview. **CVE ID : CVE-2021-25447**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=8	H-SAM-SMAR-180821/502
secomea					
sitemanager					
Incorrect Authorization	05-Aug-21	2.1	Improper Access Control vulnerability in web service of Secomea SiteManager allows local attacker without	https://www.secomea.com/support/cybersecurity-	H-SEC-SITE-180821/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials to gather network information and configuration of the SiteManager. This issue affects: Secomea SiteManager All versions prior to 9.5 on Hardware. **CVE ID : CVE-2021-32002**	advisory	
Insufficiently Protected Credentials	05-Aug-21	2.1	Unprotected Transport of Credentials vulnerability in SiteManager provisioning service allows local attacker to capture credentials if the service is used after provisioning. This issue affects: Secomea SiteManager All versions prior to 9.5 on Hardware. **CVE ID : CVE-2021-32003**	https://www.secomea.com/support/cybersecurity-advisory	H-SEC-SITE-180821/504
Sonicwall					
sma_210					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-21	7.5	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of a SQL Command leading to SQL Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products, specifically the SRA appliances running all 8.x firmware and 9.0.0.9-26sv or earlier. **CVE ID : CVE-2021-20028**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0017	H-SON-SMA_-180821/505
sma_410					
Improper Neutralization of Special Elements	04-Aug-21	7.5	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of a SQL Command leading to SQL	https://psirt.global.sonicwall.com/vuln-detail/SNWL	H-SON-SMA_-180821/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products, specifically the SRA appliances running all 8.x firmware and 9.0.0.9-26sv or earlier. **CVE ID : CVE-2021-20028**	ID-2021-0017	
sma_500v					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-21	7.5	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of a SQL Command leading to SQL Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products, specifically the SRA appliances running all 8.x firmware and 9.0.0.9-26sv or earlier. **CVE ID : CVE-2021-20028**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0017	H-SON-SMA_-180821/507
swisslog-healthcare					
hmi-3_control_panel					
Improper Verification of Cryptographic Signature	02-Aug-21	7.5	A firmware validation issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. There is no firmware validation (e.g., cryptographic signature validation) during a File Upload for a firmware update. **CVE ID : CVE-2021-37160**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulne	H-SWI-HMI--180821/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				rability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Aug-21	7.5	A buffer overflow issue was discovered in the HMI3 Control Panel contained within the Swisslog Healthcare Nexus Panel, operated by released versions of software before Nexus Software 7.2.5.7. A buffer overflow allows an attacker to overwrite an internal queue data structure and can lead to remote code execution. **CVE ID : CVE-2021-37161**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	H-SWI-HMI--180821/509
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Aug-21	7.5	A buffer overflow issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. If an attacker sends a malformed UDP message, a buffer underflow occurs,	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-	H-SWI-HMI--180821/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to an out-of-bounds copy and possible remote code execution. **CVE ID : CVE-2021-37162**	disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	
Use of Hard-coded Credentials	02-Aug-21	7.5	An insecure permissions issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus operated by released versions of software before Nexus Software 7.2.5.7. The device has two user accounts with passwords that are hardcoded. **CVE ID : CVE-2021-37163**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	H-SWI-HMI--180821/511
Out-of-bounds Write	02-Aug-21	7.5	A buffer overflow issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by	https://www.swisslog-healthcare.com/en-	H-SWI-HMI--180821/512

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
			released versions of software before Nexus Software 7.2.5.7. In the tcpTxThread function, the received data is copied to a stack buffer. An off-by-3 condition can occur, resulting in a stack-based buffer overflow. **CVE ID : CVE-2021-37164**	us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Aug-21	7.5	A buffer overflow issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. When a message is sent to the HMI TCP socket, it is forwarded to the hmiProcessMsg function through the pendingQ, and may lead to remote code execution. **CVE ID : CVE-2021-37165**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%	H-SWI-HMI--180821/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				20	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Aug-21	7.8	A buffer overflow issue leading to denial of service was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. When HMI3 starts up, it binds a local service to a TCP port on all interfaces of the device, and takes extensive time for the GUI to connect to the TCP socket, allowing the connection to be hijacked by an external attacker. **CVE ID : CVE-2021-37166**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	H-SWI-HMI-180821/514
Incorrect Default Permissions	02-Aug-21	10	An insecure permissions issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. A user logged in using the default credentials can gain root access to the device, which provides permissions for all of the functionality of the device. **CVE ID : CVE-2021-37167**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%2	H-SWI-HMI-180821/515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				0%20CVE-2021-37164%20%204%20more%20rows%20	
totolink					
a720r					
Improper Authentication	05-Aug-21	7.5	A vulnerability in the Form_Login function of TOTOLINK A720R A720R_Firmware V4.1.5cu.470_B20200911 allows attackers to bypass authentication. **CVE ID : CVE-2021-35324**	N/A	H-TOT-A720-180821/516
Out-of-bounds Write	05-Aug-21	5	A stack overflow in the checkLoginUser function of TOTOLINK A720R A720R_Firmware v4.1.5cu.470_B20200911 allows attackers to cause a denial of service (DOS). **CVE ID : CVE-2021-35325**	N/A	H-TOT-A720-180821/517
N/A	05-Aug-21	5	A vulnerability in TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows attackers to download the configuration file via sending a crafted HTTP request. **CVE ID : CVE-2021-35326**	N/A	H-TOT-A720-180821/518
Missing Authorization	05-Aug-21	7.5	A vulnerability in TOTOLINK A720R A720R_Firmware v4.1.5cu.470_B20200911 allows attackers to start the Telnet service, then login with	N/A	H-TOT-A720-180821/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the default credentials via a crafted POST request. **CVE ID : CVE-2021-35327**		
Trendnet					
tew-755ap					
NULL Pointer Dereference	10-Aug-21	5	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key. **CVE ID : CVE-2021-28845**	N/A	H-TRE-TEW--180821/520
tew-755ap2kac					
NULL Pointer Dereference	10-Aug-21	5	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key. **CVE ID : CVE-2021-28845**	N/A	H-TRE-TEW--180821/521
tew-821dap2kac					
NULL Pointer Dereference	10-Aug-21	5	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP	N/A	H-TRE-TEW--180821/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key. **CVE ID : CVE-2021-28845**		
tew-825dap					
NULL Pointer Dereference	10-Aug-21	5	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key. **CVE ID : CVE-2021-28845**	N/A	H-TRE-TEW--180821/523
vizio					
e50x-e1					
N/A	03-Aug-21	7.2	Vizio P65-F1 6.0.31.4-2 and E50x-E1 10.0.31.4-2 Smart TVs allow a threat actor to execute arbitrary code from a USB drive via the Smart Cast functionality, because files on the USB drive are effectively under the web root and can be executed. **CVE ID : CVE-2021-27942**	N/A	H-VIZ-E50X-180821/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	02-Aug-21	5	The pairing procedure used by the Vizio P65-F1 6.0.31.4-2 and E50x-E1 10.0.31.4-2 Smart TVs and mobile application is vulnerable to a brute-force attack (against only 10000 possibilities), allowing a threat actor to forcefully pair the device, leading to remote control of the TV settings and configurations. **CVE ID : CVE-2021-27943**	https://www.vizio.com	H-VIZ-E50X-180821/525
p65-f1					
N/A	03-Aug-21	7.2	Vizio P65-F1 6.0.31.4-2 and E50x-E1 10.0.31.4-2 Smart TVs allow a threat actor to execute arbitrary code from a USB drive via the Smart Cast functionality, because files on the USB drive are effectively under the web root and can be executed. **CVE ID : CVE-2021-27942**	N/A	H-VIZ-P65--180821/526
Improper Restriction of Excessive Authentication Attempts	02-Aug-21	5	The pairing procedure used by the Vizio P65-F1 6.0.31.4-2 and E50x-E1 10.0.31.4-2 Smart TVs and mobile application is vulnerable to a brute-force attack (against only 10000 possibilities), allowing a threat actor to forcefully pair the device, leading to remote control of the TV settings and configurations. **CVE ID : CVE-2021-27943**	https://www.vizio.com	H-VIZ-P65--180821/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ZTE					
zxctn_6120h					
Insufficient Verification of Data Authenticity	05-Aug-21	2.1	A ZTE's product of the transport network access layer has a security vulnerability. Because the system does not sufficiently verify the data reliability, attackers could replace an authenticated optical module on the equipment with an unauthenticated one, bypassing system authentication and detection, thus affecting signal transmission. This affects: <ZXCTN 6120H><V5.10.00B24> **CVE ID : CVE-2021-21739**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1017024	H-ZTE-ZXCT-180821/528
zxiptv					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-21	4.3	ZTE's big video business platform has two reflective cross-site scripting (XSS) vulnerabilities. Due to insufficient input verification, the attacker could implement XSS attacks by tampering with the parameters, to affect the operations of valid users. This affects: <ZXIPTV><ZXIPTV-EAS_PV5.06.04.09> **CVE ID : CVE-2021-21738**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1016764	H-ZTE-ZXIP-180821/529
Operating System					
Apple					
iphone_os					
Incorrect	03-Aug-21	4.3	Insufficient policy	https://chro	O-APP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			enforcement in image handling in iOS in Google Chrome on iOS prior to 92.0.4515.107 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2021-30583**	mereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	IPHO-180821/530
macos					
N/A	05-Aug-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33597**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories	O-APP-MACO-180821/531
bosch					
aviotec_firmware					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	O-BOS-AVIO-180821/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**		
cpp13_firmware					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	O-BOS-CPP1-180821/533
cpp14_firmware					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	O-BOS-CPP1-180821/534
cpp4_firmware					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf	https://psirt.bosch.com/security-advisories/bosch-sa-	O-BOS-CPP4-180821/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	033305-bt.html	
cpp6_firmware					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	O-BOS-CPP6-180821/536
cpp7.3_firmware					
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	O-BOS-CPP7-180821/537
cpp7_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	05-Aug-21	6.8	A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera. **CVE ID : CVE-2021-23849**	https://psirt.bosch.com/security-advisories/bosch-sa-033305-bt.html	O-BOS-CPP7-180821/538
Cisco					
small_business_rv_series_router_firmware					
Improper Input Validation	04-Aug-21	10	A vulnerability in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges. Due to the nature of the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4	O-CIS-SMAL-180821/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, only commands without parameters can be executed. **CVE ID : CVE-2021-1602**		
N/A	04-Aug-21	10	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1609**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy	O-CIS-SMAL-180821/540
N/A	04-Aug-21	9	Multiple vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to do the following: Execute arbitrary code Cause a denial of service (DoS) condition Execute arbitrary commands For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1610**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy	O-CIS-SMAL-180821/541
Debian					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
debian_linux					
Insufficiently Protected Credentials	07-Aug-21	5	Lynx through 2.8.9 mishandles the userinfo subcomponent of a URI, which allows remote attackers to discover cleartext credentials because they may appear in SNI data. **CVE ID : CVE-2021-38165**	N/A	O-DEB-DEBI-180821/542
Dell					
emc_idrac8_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	03-Aug-21	4.3	Dell EMC iDRAC8 versions prior to 2.80.80.80 & Dell EMC iDRAC9 versions prior to 5.00.00.00 contain a Content spoofing / Text injection, where a malicious URL can inject text to present a customized message on the application that can phish users into believing that the message is legitimate. **CVE ID : CVE-2021-21580**	https://www.dell.com/support/kbdoc/000189193	O-DEL-EMC_-180821/543
emc_idrac9_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	4.3	Dell EMC iDRAC9 versions prior to 4.40.40.00 contain a DOM-based cross-site scripting vulnerability. A remote attacker could potentially exploit this vulnerability to run malicious HTML or JavaScript in a victim’s browser by tricking a victim in to following a specially crafted link. **CVE ID : CVE-2021-21576**	https://www.dell.com/support/kbdoc/000189193	O-DEL-EMC_-180821/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	4.3	Dell EMC iDRAC9 versions prior to 4.40.40.00 contain a DOM-based cross-site scripting vulnerability. A remote attacker could potentially exploit this vulnerability to run malicious HTML or JavaScript in a victim’s browser by tricking a victim in to following a specially crafted link. **CVE ID : CVE-2021-21577**	https://www.dell.com/support/kbdoc/000189193	O-DEL-EMC_-180821/545
URL Redirection to Untrusted Site ('Open Redirect')	03-Aug-21	5.8	Dell EMC iDRAC9 versions prior to 4.40.40.00 contain an open redirect vulnerability. A remote unauthenticated attacker may exploit this vulnerability to redirect users to arbitrary web URLs by tricking the victim users to click on maliciously crafted links. **CVE ID : CVE-2021-21578**	https://www.dell.com/support/kbdoc/000189193	O-DEL-EMC_-180821/546
URL Redirection to Untrusted Site ('Open Redirect')	03-Aug-21	5.8	Dell EMC iDRAC9 versions prior to 4.40.40.00 contain an open redirect vulnerability. A remote unauthenticated attacker may exploit this vulnerability to redirect users to arbitrary web URLs by tricking the victim users to click on maliciously crafted links. **CVE ID : CVE-2021-21579**	https://www.dell.com/support/kbdoc/000189193	O-DEL-EMC_-180821/547
Improper Neutralization of Special Elements in	03-Aug-21	4.3	Dell EMC iDRAC8 versions prior to 2.80.80.80 & Dell EMC iDRAC9 versions prior to 5.00.00.00 contain a Content	https://www.dell.com/support/kbdoc/	O-DEL-EMC_-180821/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output Used by a Downstream Component ('Injection')			spoofing / Text injection, where a malicious URL can inject text to present a customized message on the application that can phish users into believing that the message is legitimate. **CVE ID : CVE-2021-21580**	000189193	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-21	4.3	Dell EMC iDRAC9 versions prior to 5.00.00.00 contain a cross-site scripting vulnerability. A remote attacker could potentially exploit this vulnerability to run malicious HTML or JavaScript in a victim's browser by tricking a victim in to following a specially crafted link. **CVE ID : CVE-2021-21581**	https://www.dell.com/support/kbdoc/000189193	O-DEL-EMC_-180821/549
emc_powerscale_onefs					
Untrusted Search Path	03-Aug-21	2.1	Dell EMC PowerScale OneFS contains an untrusted search path vulnerability. This vulnerability allows a user with (ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE) and (ISI_PRIV_SYS_UPGRADE or ISI_PRIV_AUDIT) to provide an untrusted path which can lead to run resources that are not under the application's direct control. **CVE ID : CVE-2021-21562**	https://www.dell.com/support/kbdoc/000188148	O-DEL-EMC_-180821/550
Improper Check for	03-Aug-21	4	Dell EMC PowerScale OneFS versions 8.1.2-9.1.0.x contain	https://www.dell.com/sup	O-DEL-EMC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			an Improper Check for Unusual or Exceptional Conditions in its auditing component.This can lead to an authenticated user with low-privileges to trigger a denial of service event. **CVE ID : CVE-2021-21563**	port/kbdoc/000188148	180821/551
Dlink					
dir-615_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Aug-21	7.5	A buffer overflow in D-Link DIR-615 C2 3.03WW. The ping_ipaddr parameter in ping_response.cgi POST request allows an attacker to crash the webserver and might even gain remote code execution. **CVE ID : CVE-2021-37388**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--180821/552
ecobee					
ecobee3_lite_firmware					
Use of Hard-coded Credentials	03-Aug-21	5	Hardcoded default root credentials exist on the ecobee3 lite 4.5.81.200 device. This allows a threat actor to gain access to the password-protected bootloader environment through the serial console. **CVE ID : CVE-2021-27952**	N/A	O-ECO-ECOB-180821/553
NULL Pointer Dereference	03-Aug-21	7.8	A NULL pointer dereference vulnerability exists on the ecobee3 lite 4.5.81.200 device in the HomeKit Wireless Access Control setup process. A threat actor can exploit this	N/A	O-ECO-ECOB-180821/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to cause a denial of service, forcing the device to reboot via a crafted HTTP request. **CVE ID : CVE-2021-27953**		
Out-of-bounds Write	03-Aug-21	6.4	A heap-based buffer overflow vulnerability exists on the ecobee3 lite 4.5.81.200 device in the HKProcessConfig function of the HomeKit Wireless Access Control setup process. A threat actor can exploit this vulnerability to force the device to connect to a SSID or cause a denial of service. **CVE ID : CVE-2021-27954**	N/A	O-ECO-ECOB-180821/555
Fedoraproject					
fedora					
Insufficiently Protected Credentials	05-Aug-21	2.6	When curl is instructed to get content using the metalink feature, and a user name and password are used to download the metalink XML file, those same credentials are then subsequently passed on to each of the servers from which curl will download or try to download the contents from. Often contrary to the user's expectations and intentions and without telling the user it happened. **CVE ID : CVE-2021-22923**	N/A	O-FED-FEDO-180821/556
Concurrent Execution using Shared	02-Aug-21	6.8	crossbeam-deque is a package of work-stealing deques for building task schedulers when	https://github.com/crossbeam-	O-FED-FEDO-180821/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			programming in Rust. In versions prior to 0.7.4 and 0.8.0, the result of the race condition is that one or more tasks in the worker queue can be popped twice instead of other tasks that are forgotten and never popped. If tasks are allocated on the heap, this can cause double free and a memory leak. If not, this still can cause a logical bug. Crates using `Stealer::steal`, `Stealer::steal_batch`, or `Stealer::steal_batch_and_pop` are affected by this issue. This has been fixed in crossbeam-deque 0.8.1 and 0.7.4. **CVE ID : CVE-2021-32810**	rs/crossbeam/security/advisories/GHSA-pqqp-xmhj-wgcw	
Observable Discrepancy	02-Aug-21	2.1	In the Linux kernel through 5.13.7, an unprivileged BPF program can obtain sensitive information from kernel memory via a Speculative Store Bypass side-channel attack because the protection mechanism neglects the possibility of uninitialized memory locations on the BPF stack. **CVE ID : CVE-2021-34556**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=f5e81d1117501546b7be050c5fbafa6efd2c722c, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=2039f26f3aca5b0e419b98f65dd36481337b86ee	O-FED-FEDO-180821/558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	02-Aug-21	2.1	In the Linux kernel through 5.13.7, an unprivileged BPF program can obtain sensitive information from kernel memory via a Speculative Store Bypass side-channel attack because a certain preempting store operation does not necessarily occur before a store operation that has an attacker-controlled value. **CVE ID : CVE-2021-35477**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=f5e81d1117501546b7be050c5fbafa6efd2c722c, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=2039f26f3aca5b0e419b98f65dd36481337b86ee	O-FED-FEDO-180821/559
Fortinet					
fortios					
N/A	04-Aug-21	5.8	A buffer underwrite vulnerability in the firmware verification routine of FortiOS before 7.0.1 may allow an attacker located in the adjacent network to potentially execute arbitrary code via a specifically crafted firmware image. **CVE ID : CVE-2021-24018**	https://fortiguard.com/advisory/FG-IR-21-046	O-FOR-FORT-180821/560
Google					
android					
Use After Free	05-Aug-21	4.6	A use after free vulnerability in conn_gadget driver prior to SMR AUG-2021 Release 1	https://security.samsungmobile.com/	O-GOO-ANDR-180821/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows malicious action by an attacker. **CVE ID : CVE-2021-25443**	securityUpdate.smsb?year=2021&month=8	
N/A	05-Aug-21	2.1	An IV reuse vulnerability in keymaster prior to SMR AUG-2021 Release 1 allows decryption of custom keyblob with privileged process. **CVE ID : CVE-2021-25444**	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=8	O-GOO-ANDR-180821/562
chrome_os					
Out-of-bounds Write	03-Aug-21	6.8	Out of bounds write in Tab Groups in Google Chrome on Linux and ChromeOS prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page. **CVE ID : CVE-2021-30565**	https://crbug.com/1210985, https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	O-GOO-CHRO-180821/563
Huawei					
ecns280_td_firmware					
Improper Privilege Management	02-Aug-21	4.6	There is a privilege escalation vulnerability in some Huawei products. Due to improper privilege management, a local attacker with common privilege may access some specific files in the affected products. Successful exploit will cause privilege escalation.Affected product versions include:eCNS280_TD V100R005C00,V100R005C10;	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-privilege-en	O-HUA-ECNS-180821/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			eSE620X vESS V100R001C10SPC200,V100R001C20SPC200. **CVE ID : CVE-2021-22396**		
emui					
Integer Underflow (Wrap or Wraparound)	02-Aug-21	5	There is an Integer Underflow (Wrap or Wraparound) Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause DoS of Samgr. **CVE ID : CVE-2021-22379**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/565
Improper Input Validation	02-Aug-21	5	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause an infinite loop in DoS. **CVE ID : CVE-2021-22381**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/566
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Aug-21	6.8	There is an Information Disclosure Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to authentication bypass. **CVE ID : CVE-2021-22384**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/567
Improper Control of Dynamically-Managed Code Resources	02-Aug-21	7.5	There is an Improper Control of Dynamically Managing Code Resources Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to remotely execute	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands. **CVE ID : CVE-2021-22387**		
Integer Overflow or Wraparound	02-Aug-21	7.5	There is an Integer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause certain codes to be executed. **CVE ID : CVE-2021-22388**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/569
Incorrect Authorization	02-Aug-21	7.5	There is a Permission Control Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause certain codes to be executed. **CVE ID : CVE-2021-22389**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/570
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Aug-21	7.5	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause certain codes to be executed. **CVE ID : CVE-2021-22390**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/571
Incorrect Calculation of Buffer Size	02-Aug-21	5	There is an Incorrect Calculation of Buffer Size in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22391**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/572
Incorrect Calculation of Buffer Size	02-Aug-21	5	There is an Incorrect Calculation of Buffer Size in Huawei Smartphone.Successful	https://consumer.huawei.com/en/support/bulletin	O-HUA-EMUI-180821/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may cause verification bypass and directions to abnormal addresses. **CVE ID : CVE-2021-22392**	/2021/6/	
Integer Overflow or Wraparound	02-Aug-21	5	There is an Integer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause random kernel address access. **CVE ID : CVE-2021-22412**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/574
Out-of-bounds Write	02-Aug-21	5	There is an Integer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22413**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/575
Out-of-bounds Write	02-Aug-21	5	There is a Memory Buffer Errors Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22414**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/576
Incorrect Calculation of Buffer Size	02-Aug-21	5	There is an Incorrect Calculation of Buffer Size Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause kernel exceptions with the code.	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22415		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Aug-21	6.8	There is a Heap-based Buffer Overflow Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to authentication bypass. **CVE ID : CVE-2021-22427**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/578
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Aug-21	6.8	There is an Incomplete Cleanup Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to authentication bypass. **CVE ID : CVE-2021-22428**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/579
N/A	02-Aug-21	6.4	There is a Configuration Defect Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service integrity and availability. **CVE ID : CVE-2021-22435**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/580
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Aug-21	7.5	There is a Memory Buffer Improper Operation Limit Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause malicious code to be executed. **CVE ID : CVE-2021-22438**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/581
Improper	02-Aug-21	5	There is an Improper	https://cons	O-HUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Integrity Check Value			Validation of Integrity Check Value Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause the system to reset. **CVE ID : CVE-2021-22442**	umer.huawei.com/en/support/bulletin/2021/6/	EMUI-180821/582
Improper Input Validation	02-Aug-21	5	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause random address access. **CVE ID : CVE-2021-22443**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/583
Improper Input Validation	02-Aug-21	7.5	There is an Input Verification Vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause code injection. **CVE ID : CVE-2021-22444**	https://consumer.huawei.com/en/support/bulletin/2021/6/	O-HUA-EMUI-180821/584
ese620x_vess_firmware					
Improper Privilege Management	02-Aug-21	4.6	There is a privilege escalation vulnerability in some Huawei products. Due to improper privilege management, a local attacker with common privilege may access some specific files in the affected products. Successful exploit will cause privilege escalation.Affected product versions include:eCNS280_TD V100R005C00,V100R005C10; eSE620X vESS V100R001C10SPC200,V100R001C20SPC200.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-privilege-en	O-HUA-ESE6-180821/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22396		
harmonyos					
Incorrect Default Permissions	06-Aug-21	2.1	A component of the HarmonyOS has a permission bypass vulnerability. Local attackers may exploit this vulnerability to cause the device to hang due to the page error OsVmPageFaultHandler. **CVE ID : CVE-2021-22295**	https://device.harmonyos.com/cn/console/safetyDetail?id=9145efa5d9064d94a7fc3968b6054d83&pageSize=10&pageIndex=1	O-HUA-HARM-180821/586
N/A	03-Aug-21	7.2	A component of the HarmonyOS has a Data Processing Errors vulnerability. Local attackers may exploit this vulnerability to cause Kernel Code Execution. **CVE ID : CVE-2021-22416**	https://device.harmonyos.com/cn/docs/security/update/oem_security_update_phone_202106-0000001165452077	O-HUA-HARM-180821/587
N/A	03-Aug-21	4.9	A component of the HarmonyOS has a Data Processing Errors vulnerability. Local attackers may exploit this vulnerability to cause Kernel Memory Leakage. **CVE ID : CVE-2021-22417**	https://device.harmonyos.com/cn/docs/security/update/oem_security_update_phone_202106-0000001165452077	O-HUA-HARM-180821/588
Integer Overflow or Wraparound	03-Aug-21	7.2	A component of the HarmonyOS has a Integer Overflow or Wraparound vulnerability. Local attackers may exploit this vulnerability to cause memory overwriting.	https://device.harmonyos.com/cn/docs/security/update/oem_security_updat	O-HUA-HARM-180821/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22418	e_phone_202106-0000001165452077	
Insufficient Verification of Data Authenticity	03-Aug-21	4.9	A component of the HarmonyOS has a Insufficient Verification of Data Authenticity vulnerability. Local attackers may exploit this vulnerability to cause persistent dos. **CVE ID : CVE-2021-22419**	https://device.harmonyos.com/cn/docs/security/update/oem_security_update_phone_202106-0000001165452077	O-HUA-HARM-180821/590
Externally Controlled Reference to a Resource in Another Sphere	03-Aug-21	7.2	A component of the HarmonyOS has a External Control of System or Configuration Setting vulnerability. Local attackers may exploit this vulnerability to cause the underlying trust of the application trustlist mechanism is missing.. **CVE ID : CVE-2021-22420**	https://device.harmonyos.com/cn/docs/security/update/oem_security_update_phone_202106-0000001165452077	O-HUA-HARM-180821/591
Improper Privilege Management	03-Aug-21	7.2	A component of the HarmonyOS has a Improper Privilege Management vulnerability. Local attackers may exploit this vulnerability to cause further Elevation of Privileges. **CVE ID : CVE-2021-22421**	https://device.harmonyos.com/cn/docs/security/update/oem_security_update_phone_202106-0000001165452077	O-HUA-HARM-180821/592
Integer Overflow or Wraparound	03-Aug-21	7.2	A component of the HarmonyOS has a Integer Overflow or Wraparound vulnerability. Local attackers	https://device.harmonyos.com/cn/docs/security/up	O-HUA-HARM-180821/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may exploit this vulnerability to cause memory overwriting. **CVE ID : CVE-2021-22422**	date/oem_security_update_phone_202106-0000001165452077	
Out-of-bounds Write	03-Aug-21	7.2	A component of the HarmonyOS has a Out-of-bounds Write Vulnerability. Local attackers may exploit this vulnerability to cause integer overflow. **CVE ID : CVE-2021-22423**	https://device.harmonyos.com/cn/docs/security/update/oem_security_update_phone_202106-0000001165452077	O-HUA-HARM-180821/594
Missing Release of Memory after Effective Lifetime	03-Aug-21	4.9	A component of the HarmonyOS has a Kernel Memory Leakage Vulnerability. Local attackers may exploit this vulnerability to cause Kernel Denial of Service. **CVE ID : CVE-2021-22424**	https://device.harmonyos.com/cn/docs/security/update/oem_security_update_phone_202106-0000001165452077	O-HUA-HARM-180821/595
Double Free	03-Aug-21	7.2	A component of the HarmonyOS has a Double Free vulnerability. Local attackers may exploit this vulnerability to cause Root Elevating Privileges. **CVE ID : CVE-2021-22425**	https://device.harmonyos.com/cn/docs/security/update/oem_security_update_phone_202106-0000001165452077	O-HUA-HARM-180821/596
hulk-al00c_firmware					
Incorrect	02-Aug-21	2.1	There is a logic error	https://www	O-HUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations. Affected product versions include: Hulk-AL00C 9.1.1.201(C00E201R8P1);Jennifer-AN00C 10.1.1.171(C00E170R6P3);Jenny-AL10B 10.1.0.228(C00E220R5P1) and OxfordPL-AN10B 10.1.0.116(C00E110R2P1). **CVE ID : CVE-2021-22398**	.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-smartphone-en	HULK-180821/597
jennifer-an00c_firmware					
Incorrect Authorization	02-Aug-21	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations. Affected product versions include: Hulk-AL00C 9.1.1.201(C00E201R8P1);Jennifer-AN00C 10.1.1.171(C00E170R6P3);Jenny-AL10B 10.1.0.228(C00E220R5P1) and OxfordPL-AN10B	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-smartphone-en	O-HUA-JENN-180821/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.116(C00E110R2P1). **CVE ID : CVE-2021-22398**		
jenny-al10b_firmware					
Incorrect Authorization	02-Aug-21	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations. Affected product versions include: Hulk-AL00C 9.1.1.201(C00E201R8P1);Jennifer-AN00C 10.1.1.171(C00E170R6P3);Jenny-AL10B 10.1.0.228(C00E220R5P1) and OxfordPL-AN10B 10.1.0.116(C00E110R2P1). **CVE ID : CVE-2021-22398**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-smartphone-en	O-HUA-JENN-180821/599
oxfordpl-an10b_firmware					
Incorrect Authorization	02-Aug-21	2.1	There is a logic error vulnerability in several smartphones. The software does not properly restrict certain operation when the Digital Balance function is on. Successful exploit could allow the attacker to bypass the Digital Balance limit after a series of operations. Affected product versions include: Hulk-AL00C 9.1.1.201(C00E201R8P1);Jennifer-AN00C	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210714-01-smartphone-en	O-HUA-OXFO-180821/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.1.171(C00E170R6P3);Jenny-AL10B 10.1.0.228(C00E220R5P1) and OxfordPL-AN10B 10.1.0.116(C00E110R2P1). **CVE ID : CVE-2021-22398**		
oxfords-an00a_firmware					
Improper Input Validation	03-Aug-21	4.3	Some Huawei Smartphones has an insufficient input validation vulnerability due to the lack of parameter validation. An attacker may trick a user into installing a malicious APP. The app can modify specific parameters, causing the system to crash. Affected product include:OxfordS-AN00A 10.0.1.10(C00E10R1P1),10.0.1.105(C00E103R3P3),10.0.1.115(C00E110R3P3),10.0.1.123(C00E121R3P3),10.0.1.135(C00E130R3P3),10.0.1.135(C00E130R4P1),10.0.1.152(C00E140R4P1),10.0.1.160(C00E160R4P1),10.0.1.167(C00E166R4P1),10.0.1.173(C00E172R5P1),10.0.1.178(C00E175R5P1) and 10.1.0.202(C00E79R5P1). **CVE ID : CVE-2021-22400**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210721-01-phones-en	O-HUA-OXFO-180821/601
IBM					
aix					
Improper Privilege Management	02-Aug-21	7.2	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a local user to exploit a vulnerability in Korn Shell (ksh) to gain root privileges. IBM X-Force ID:	https://www.ibm.com/support/pages/node/6477018	O-IBM-AIX-180821/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			201478. **CVE ID : CVE-2021-29741**		
powervm					
Improper Authentication	04-Aug-21	5	IBM PowerVM Hypervisor FW940 and FW950 could allow an attacker to obtain sensitive information if they gain service access to the FSP. IBM X-Force ID: 202476. **CVE ID : CVE-2021-29765**	https://www.ibm.com/support/pages/node/6478039, https://exchange.xforce.ibmcloud.com/vulnerabilities/202476	O-IBM-POWE-180821/603
vios					
Improper Privilege Management	02-Aug-21	7.2	IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a local user to exploit a vulnerability in Korn Shell (ksh) to gain root privileges. IBM X-Force ID: 201478. **CVE ID : CVE-2021-29741**	https://www.ibm.com/support/pages/node/6477018	O-IBM-VIOS-180821/604
Linux					
linux_kernel					
Out-of-bounds Write	03-Aug-21	6.8	Out of bounds write in Tab Groups in Google Chrome on Linux and ChromeOS prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page. **CVE ID : CVE-2021-30565**	https://crbug.com/1210985, https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html	O-LIN-LINU-180821/605
Observable	02-Aug-21	2.1	In the Linux kernel through	https://git.ke	O-LIN-LINU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Discrepancy			5.13.7, an unprivileged BPF program can obtain sensitive information from kernel memory via a Speculative Store Bypass side-channel attack because the protection mechanism neglects the possibility of uninitialized memory locations on the BPF stack. **CVE ID : CVE-2021-34556**	rnel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=f5e81d1117501546b7be050c5fbafa6efd2c722c, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=2039f26f3aca5b0e419b98f65dd36481337b86ee	180821/606
Observable Discrepancy	02-Aug-21	2.1	In the Linux kernel through 5.13.7, an unprivileged BPF program can obtain sensitive information from kernel memory via a Speculative Store Bypass side-channel attack because a certain preempting store operation does not necessarily occur before a store operation that has an attacker-controlled value. **CVE ID : CVE-2021-35477**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=f5e81d1117501546b7be050c5fbafa6efd2c722c, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=2039f26f3aca5b0e419b98f65dd36481337b86ee	O-LIN-LINU-180821/607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Initialization of Resource	05-Aug-21	2.1	A vulnerability was found in the Linux kernel in versions before v5.14-rc1. Missing size validations on inbound SCTP packets may allow the kernel to read uninitialized memory. **CVE ID : CVE-2021-3655**	https://bugzilla.redhat.com/show_bug.cgi?id=1984024	O-LIN-LINU-180821/608
Uncontrolled Resource Consumption	05-Aug-21	2.1	A lack of CPU resource in the Linux kernel tracing module functionality in versions prior to 5.14-rc3 was found in the way user uses trace ring buffer in a specific way. Only privileged local users (with CAP_SYS_ADMIN capability) could use this flaw to starve the resources causing denial of service. **CVE ID : CVE-2021-3679**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=67f0d6d9883c13174669f88adac4f0ee656cc16a, https://bugzilla.redhat.com/show_bug.cgi?id=1989165	O-LIN-LINU-180821/609
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-21	7.2	In drivers/char/virtio_console.c in the Linux kernel before 5.13.4, data corruption or loss can be triggered by an untrusted device that supplies a buf->len value exceeding the buffer size. **CVE ID : CVE-2021-38160**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.4, https://github.com/torvalds/linux/commit/d00d8da5869a2608e97cfede094dfc5e11462a46	O-LIN-LINU-180821/610
Out-of-bounds Write	07-Aug-21	4.6	In kernel/bpf/hashtab.c in the Linux kernel through 5.13.8, there is an integer overflow	https://lore.kernel.org/bpf/20210806	O-LIN-LINU-180821/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and out-of-bounds write when many elements are placed in a single bucket. NOTE: exploitation might be impractical without the CAP_SYS_ADMIN capability. **CVE ID : CVE-2021-38166**	150419.109658-1-th.yasumatsu@gmail.com/ , https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf.git/commit/?id=c4eb1f403243fc7bbb7de644db8587c03de36da6	
N/A	08-Aug-21	2.1	arch/x86/kvm/mmu/paging_tmpl.h in the Linux kernel before 5.12.11 incorrectly computes the access permissions of a shadow page, leading to a missing guest protection page fault. **CVE ID : CVE-2021-38198**	https://github.com/torvalds/linux/commit/b1bd5cba3306691c771d558e94baa73e8b0b96b7, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.11	O-LIN-LINU-180821/612
N/A	08-Aug-21	5	fs/nfs/nfs4client.c in the Linux kernel before 5.13.4 has incorrect connection-setup ordering, which allows operators of remote NFSv4 servers to cause a denial of service (hanging of mounts) by arranging for those servers to be unreachable during trunking detection.	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.4, https://github.com/torvalds/linux/commit/dd99e9f98fbf423ff	O-LIN-LINU-180821/613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-38199	6d365b37a98e8879170f17c	
NULL Pointer Dereference	08-Aug-21	2.1	arch/powerpc/perf/core-book3s.c in the Linux kernel before 5.12.13, on systems with perf_event_paranoid=-1 and no specific PMU driver support registered, allows local users to cause a denial of service (perf_instruction_pointer NULL pointer dereference and OOPS) via a "perf record" command. **CVE ID : CVE-2021-38200**	https://github.com/torvalds/linux/commit/60b7ed54a41b550d50caf7f2418db4a7e75b5bdc, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.13	O-LIN-LINU-180821/614
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Aug-21	5	net/sunrpc/xdr.c in the Linux kernel before 5.13.4 allows remote attackers to cause a denial of service (xdr_set_page_base slab-out-of-bounds access) by performing many NFS 4.2 READ_PLUS operations. **CVE ID : CVE-2021-38201**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.4, https://github.com/torvalds/linux/commit/6d1c0f3d28f98ea2736128ed3e46821496dc3a8c	O-LIN-LINU-180821/615
Out-of-bounds Read	08-Aug-21	5	fs/nfsd/trace.h in the Linux kernel before 5.13.4 might allow remote attackers to cause a denial of service (out-of-bounds read in strlen) by sending NFS traffic when the trace event framework is being used for nfsd.	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.4, https://github.com/torvalds/linux/commit/7b08cf	O-LIN-LINU-180821/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-38202	62b1239a4322427d677ea9363f0ab677c6	
Allocation of Resources Without Limits or Throttling	08-Aug-21	2.1	btrfs in the Linux kernel before 5.13.4 allows attackers to cause a denial of service (deadlock) via processes that trigger allocation of new system chunks during times when there is a shortage of free space in the system space_info. **CVE ID : CVE-2021-38203**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.4, https://github.com/torvalds/linux/commit/1cb3db1cf383a3c7dbda1aa0ce748b0958759947	O-LIN-LINU-180821/617
Use After Free	08-Aug-21	2.1	drivers/usb/host/max3421-hcd.c in the Linux kernel before 5.13.6 allows physically proximate attackers to cause a denial of service (use-after-free and panic) by removing a MAX-3421 USB device in certain situations. **CVE ID : CVE-2021-38204**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.6, https://github.com/torvalds/linux/commit/b5fdf5c6e6bee35837e160c00ac89327bdad031b	O-LIN-LINU-180821/618
Access of Uninitialized Pointer	08-Aug-21	2.1	drivers/net/ethernet/xilinx/xilinx_emaclite.c in the Linux kernel before 5.13.3 makes it easier for attackers to defeat an ASLR protection mechanism because it prints a kernel pointer (i.e., the real IOMEM pointer).	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.3, https://github.com/torvalds/linux/commit/d0d62	O-LIN-LINU-180821/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-38205	baa7f505bd4c59cd169692ff07ec49dde37	
NULL Pointer Dereference	08-Aug-21	2.1	The mac80211 subsystem in the Linux kernel before 5.12.13, when a device supporting only 5 GHz is used, allows attackers to cause a denial of service (NULL pointer dereference in the radiotap parser) by injecting a frame with 802.11a rates. **CVE ID : CVE-2021-38206**	https://github.com/torvalds/linux/commit/bddc0c411a45d3718ac535a070f349be8eca8d48, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.13	O-LIN-LINU-180821/620
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Aug-21	5	drivers/net/ethernet/xilinx/ll_temac_main.c in the Linux kernel before 5.12.13 allows remote attackers to cause a denial of service (buffer overflow and lockup) by sending heavy network traffic for about ten minutes. **CVE ID : CVE-2021-38207**	https://github.com/torvalds/linux/commit/c364df2489b8ef2f5e3159b1dff1f1fdb16040d, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.13	O-LIN-LINU-180821/621
NULL Pointer Dereference	08-Aug-21	2.1	net/nfc/llcp_sock.c in the Linux kernel before 5.12.10 allows local unprivileged users to cause a denial of service (NULL pointer dereference and BUG) by making a getsockname call after a certain type of failure	https://github.com/torvalds/linux/commit/4ac06a1e013cf5fdd963317ffd3b968560f33bba,	O-LIN-LINU-180821/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of a bind call. **CVE ID : CVE-2021-38208**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.10	
Observable Discrepancy	08-Aug-21	2.1	net/netfilter/nf_conntrack_standalone.c in the Linux kernel before 5.12.2 allows observation of changes in any net namespace because these changes are leaked into all other net namespaces. This is related to the NF_SYSCTL_CT_MAX, NF_SYSCTL_CT_EXPECT_MAX, and NF_SYSCTL_CT_BUCKETS sysctls. **CVE ID : CVE-2021-38209**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.2, https://github.com/torvalds/linux/commit/2671fa4dc0109d3fb581bc3078fdf17b5d9080f6	O-LIN-LINU-180821/623
Microsoft					
windows					
Improper Input Validation	05-Aug-21	7.5	An improper input validation vulnerability in the service of ezPDFReader allows attacker to execute arbitrary command. This issue occurred when the ezPDF launcher received and executed crafted input values through JSON-RPC communication. **CVE ID : CVE-2021-26605**	N/A	O-MIC-WIND-180821/624
Improper Input Validation	06-Aug-21	10	A vulnerability in PKI Security Solution of Dream Security could allow arbitrary command execution. This vulnerability is due to insufficient validation of the	N/A	O-MIC-WIND-180821/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization certificate. An attacker could exploit this vulnerability by sending a crafted HTTP request an affected program. A successful exploit could allow the attacker to remotely execute arbitrary code on a target system. **CVE ID : CVE-2021-26606**		
N/A	05-Aug-21	4.3	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the SAVAPI component used in certain F-Secure products can crash while scanning fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33597**	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories	O-MIC-WIND-180821/626
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.4.37651. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Document objects. The issue results from the	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13741. **CVE ID : CVE-2021-34831**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the delay property. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13928. **CVE ID : CVE-2021-34832**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/628
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14023. **CVE ID : CVE-2021-34833**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14014. **CVE ID : CVE-2021-34834**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/630
Use After	04-Aug-21	6.8	This vulnerability allows	https://www	O-MIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14015. **CVE ID : CVE-2021-34835**	.foxit.com/support/security-bulletins.html	WIND-180821/631
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the current process. Was ZDI-CAN-14017. **CVE ID : CVE-2021-34836**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14018. **CVE ID : CVE-2021-34837**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/633
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14019. **CVE ID : CVE-2021-34838**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14020. **CVE ID : CVE-2021-34839**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/635
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/636

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
			exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14021. **CVE ID : CVE-2021-34840**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14022. **CVE ID : CVE-2021-34841**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14024. **CVE ID : CVE-2021-34842**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/638
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14025. **CVE ID : CVE-2021-34843**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14033. **CVE ID : CVE-2021-34844**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/640
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. 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.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14034. **CVE ID : CVE-2021-34845**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14120. **CVE ID : CVE-2021-34846**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/642
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User	https://www.foxit.com/support/security-bulletins.htm	O-MIC-WIND-180821/643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14270. **CVE ID : CVE-2021-34847**	l	
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14532.	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34848		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14531. **CVE ID : CVE-2021-34849**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/645
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14529. **CVE ID : CVE-2021-34850**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14016. **CVE ID : CVE-2021-34851**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/647
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13929. **CVE ID : CVE-2021-34852**		
Use After Free	04-Aug-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.0.0.49893. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14013. **CVE ID : CVE-2021-34853**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180821/649
Uncontrolled Search Path Element	11-Aug-21	4.4	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows DLL hijacking, aka	https://www.foxitsoftware.com/support/security-	O-MIC-WIND-180821/650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CNVD-C-2021-68000 and CNVD-C-2021-68502. **CVE ID : CVE-2021-38571**	bulletins.php	
openplcproject					
openplc_v3_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Aug-21	9	Command Injection in Open PLC Webserver v3 allows remote attackers to execute arbitrary code via the "Hardware Layer Code Box" component on the "/hardware" page of the application. **CVE ID : CVE-2021-31630**	N/A	O-OPE-OPEN-180821/651
prolink					
prc2402m_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Aug-21	7.5	In ProLink PRC2402M V1.0.18 and older, the set_TR069 function in the adm.cgi binary, accessible with a page parameter value of TR069 contains a trivial command injection where the value of the TR069_local_port parameter is passed directly to system. **CVE ID : CVE-2021-36705**	N/A	O-PRO-PRC2-180821/652
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Aug-21	7.5	In ProLink PRC2402M V1.0.18 and older, the set_sys_cmd function in the adm.cgi binary, accessible with a page parameter value of sysCMD contains a trivial command injection where the value of the command parameter is passed directly to system.	N/A	O-PRO-PRC2-180821/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36706		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Aug-21	7.5	In ProLink PRC2402M V1.0.18 and older, the set_ledonoff function in the adm.cgi binary, accessible with a page parameter value of ledonoff contains a trivial command injection where the value of the led_cmd parameter is passed directly to do_system. **CVE ID : CVE-2021-36707**	N/A	O-PRO-PRC2-180821/654
Weak Password Recovery Mechanism for Forgotten Password	06-Aug-21	5	In ProLink PRC2402M V1.0.18 and older, the set_sys_init function in the login.cgi binary allows an attacker to reset the password to the administrative interface of the router. **CVE ID : CVE-2021-36708**	N/A	O-PRO-PRC2-180821/655
qsan					
xn8008t_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-21	4.3	QSAN Storage Manager header page parameters does not filter special characters. Remote attackers can inject JavaScript without logging in and launch reflected XSS attacks to access and modify specific data. **CVE ID : CVE-2021-37216**	N/A	O-QSA-XN80-180821/656
xn8024r_firmware					
Improper Neutralization of Input During Web Page	02-Aug-21	4.3	QSAN Storage Manager header page parameters does not filter special characters. Remote attackers can inject JavaScript without logging in	N/A	O-QSA-XN80-180821/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			and launch reflected XSS attacks to access and modify specific data. **CVE ID : CVE-2021-37216**		
Redhat					
enterprise_linux					
Improper Input Validation	05-Aug-21	5	A flaw was found in the way nettle's RSA decryption functions handled specially crafted ciphertext. An attacker could use this flaw to provide a manipulated ciphertext leading to application crash and denial of service. **CVE ID : CVE-2021-3580**	https://bugzilla.redhat.com/show_bug.cgi?id=1967983	O-RED-ENTE-180821/658
Missing Initialization of Resource	05-Aug-21	2.1	A vulnerability was found in the Linux kernel in versions before v5.14-rc1. Missing size validations on inbound SCTP packets may allow the kernel to read uninitialized memory. **CVE ID : CVE-2021-3655**	https://bugzilla.redhat.com/show_bug.cgi?id=1984024	O-RED-ENTE-180821/659
Uncontrolled Resource Consumption	05-Aug-21	2.1	A lack of CPU resource in the Linux kernel tracing module functionality in versions prior to 5.14-rc3 was found in the way user uses trace ring buffer in a specific way. Only privileged local users (with CAP_SYS_ADMIN capability) could use this flaw to starve the resources causing denial of service. **CVE ID : CVE-2021-3679**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=67f0d6d9883c13174669f88adac4f0ee656cc16a, https://bugzilla.redhat.com/show_bug.cgi?id=1989165	O-RED-ENTE-180821/660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release of Invalid Pointer or Reference	05-Aug-21	6.5	A flaw was found in the USB redirector device emulation of QEMU in versions prior to 6.1.0-rc2. It occurs when dropping packets during a bulk transfer from a SPICE client due to the packet queue being full. A malicious SPICE client could use this flaw to make QEMU call free() with faked heap chunk metadata, resulting in a crash of QEMU or potential code execution with the privileges of the QEMU process on the host. **CVE ID : CVE-2021-3682**	https://bugzilla.redhat.com/show_bug.cgi?id=1989651	O-RED-ENTE-180821/661
Samsung					
smartthings_firmware					
Improper Authentication	05-Aug-21	5	Improper access control vulnerability in SmartThings prior to version 1.7.67.25 allows untrusted applications to cause arbitrary webpage loading in webview. **CVE ID : CVE-2021-25446**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=8	O-SAM-SMAR-180821/662
Improper Authentication	05-Aug-21	5	Improper access control vulnerability in SmartThings prior to version 1.7.67.25 allows untrusted applications to cause local file inclusion in webview. **CVE ID : CVE-2021-25447**	https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=8	O-SAM-SMAR-180821/663
secomea					
sitemanager_firmware					
Incorrect Authorizatio	05-Aug-21	2.1	Improper Access Control vulnerability in web service of	https://www.secomea.co	O-SEC-SITE-180821/664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			Secomea SiteManager allows local attacker without credentials to gather network information and configuration of the SiteManager. This issue affects: Secomea SiteManager All versions prior to 9.5 on Hardware. **CVE ID : CVE-2021-32002**	m/support/cybersecurity-advisory	
Insufficiently Protected Credentials	05-Aug-21	2.1	Unprotected Transport of Credentials vulnerability in SiteManager provisioning service allows local attacker to capture credentials if the service is used after provisioning. This issue affects: Secomea SiteManager All versions prior to 9.5 on Hardware. **CVE ID : CVE-2021-32003**	https://www.secomea.com/support/cybersecurity-advisory	O-SEC-SITE-180821/665
Sonicwall					
sma_210_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-21	7.5	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of a SQL Command leading to SQL Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products, specifically the SRA appliances running all 8.x firmware and 9.0.0.9-26sv or earlier. **CVE ID : CVE-2021-20028**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0017	O-SON-SMA_-180821/666
sma_410_firmware					
Improper Neutralizatio	04-Aug-21	7.5	** UNSUPPORTED WHEN ASSIGNED ** Improper	https://psirt.global.sonicw	O-SON-SMA_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			neutralization of a SQL Command leading to SQL Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products, specifically the SRA appliances running all 8.x firmware and 9.0.0.9-26sv or earlier. **CVE ID : CVE-2021-20028**	all.com/vuln-detail/SNWLID-2021-0017	180821/667
sma_500v_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-21	7.5	** UNSUPPORTED WHEN ASSIGNED ** Improper neutralization of a SQL Command leading to SQL Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products, specifically the SRA appliances running all 8.x firmware and 9.0.0.9-26sv or earlier. **CVE ID : CVE-2021-20028**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0017	O-SON-SMA_-180821/668
swisslog-healthcare					
hmi-3_control_panel_firmware					
Improper Verification of Cryptographic Signature	02-Aug-21	7.5	A firmware validation issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. There is no firmware validation (e.g., cryptographic signature validation) during a File Upload for a firmware update. **CVE ID : CVE-2021-37160**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosure	O-SWI-HMI--180821/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				s%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Aug-21	7.5	A buffer overflow issue was discovered in the HMI3 Control Panel contained within the Swisslog Healthcare Nexus Panel, operated by released versions of software before Nexus Software 7.2.5.7. A buffer overflow allows an attacker to overwrite an internal queue data structure and can lead to remote code execution. **CVE ID : CVE-2021-37161**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	O-SWI-HMI--180821/670
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Aug-21	7.5	A buffer overflow issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. If an attacker sends a	https://www.swisslog-healthcare.com/en-us/customer-care/security-	O-SWI-HMI--180821/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malformed UDP message, a buffer underflow occurs, leading to an out-of-bounds copy and possible remote code execution. **CVE ID : CVE-2021-37162**	information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	
Use of Hard-coded Credentials	02-Aug-21	7.5	An insecure permissions issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus operated by released versions of software before Nexus Software 7.2.5.7. The device has two user accounts with passwords that are hardcoded. **CVE ID : CVE-2021-37163**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	O-SWI-HMI--180821/672
Out-of-bounds	02-Aug-21	7.5	A buffer overflow issue was discovered in HMI3 Control	https://www.swisslog-	O-SWI-HMI--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. In the tcpTxThread function, the received data is copied to a stack buffer. An off-by-3 condition can occur, resulting in a stack-based buffer overflow. **CVE ID : CVE-2021-37164**	healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	180821/673
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Aug-21	7.5	A buffer overflow issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. When a message is sent to the HMI TCP socket, it is forwarded to the hmiProcessMsg function through the pendingQ, and may lead to remote code execution. **CVE ID : CVE-2021-37165**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%	O-SWI-HMI--180821/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				204%20more%20rows%20	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Aug-21	7.8	A buffer overflow issue leading to denial of service was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. When HMI3 starts up, it binds a local service to a TCP port on all interfaces of the device, and takes extensive time for the GUI to connect to the TCP socket, allowing the connection to be hijacked by an external attacker. **CVE ID : CVE-2021-37166**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulnerability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	O-SWI-HMI--180821/675
Incorrect Default Permissions	02-Aug-21	10	An insecure permissions issue was discovered in HMI3 Control Panel in Swisslog Healthcare Nexus Panel operated by released versions of software before Nexus Software 7.2.5.7. A user logged in using the default credentials can gain root access to the device, which provides permissions for all of the functionality of the device. **CVE ID : CVE-2021-37167**	https://www.swisslog-healthcare.com/en-us/customer-care/security-information/cve-disclosures#:~:text=CVE%20Disclosures%20%20%20%20Vulne	O-SWI-HMI--180821/676

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
				rability%20Name%20,%20%20CVE-2021-37164%20%204%20more%20rows%20	
totolink					
a720r_firmware					
Improper Authentication	05-Aug-21	7.5	A vulnerability in the Form_Login function of TOTOLINK A720R A720R_Firmware V4.1.5cu.470_B20200911 allows attackers to bypass authentication. **CVE ID : CVE-2021-35324**	N/A	O-TOT-A720-180821/677
Out-of-bounds Write	05-Aug-21	5	A stack overflow in the checkLoginUser function of TOTOLINK A720R A720R_Firmware v4.1.5cu.470_B20200911 allows attackers to cause a denial of service (DOS). **CVE ID : CVE-2021-35325**	N/A	O-TOT-A720-180821/678
N/A	05-Aug-21	5	A vulnerability in TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows attackers to download the configuration file via sending a crafted HTTP request. **CVE ID : CVE-2021-35326**	N/A	O-TOT-A720-180821/679
Missing Authorization	05-Aug-21	7.5	A vulnerability in TOTOLINK A720R A720R_Firmware v4.1.5cu.470_B20200911	N/A	O-TOT-A720-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			allows attackers to start the Telnet service, then login with the default credentials via a crafted POST request. **CVE ID : CVE-2021-35327**		180821/680
Trendnet					
tew-755ap2kac_firmware					
NULL Pointer Dereference	10-Aug-21	5	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key. **CVE ID : CVE-2021-28845**	N/A	O-TRE-TEW--180821/681
tew-755ap_firmware					
NULL Pointer Dereference	10-Aug-21	5	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key. **CVE ID : CVE-2021-28845**	N/A	O-TRE-TEW--180821/682
tew-821dap2kac_firmware					
NULL	10-Aug-21	5	Null Pointer Dereference	N/A	O-TRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key. **CVE ID : CVE-2021-28845**		TEW--180821/683
tew-825dap_firmware					
NULL Pointer Dereference	10-Aug-21	5	Null Pointer Dereference vulnerability exists in TRENDnet TEW-755AP 1.11B03, TEW-755AP2KAC 1.11B03, TEW-821DAP2KAC 1.11B03, and TEW-825DAP 1.11B03, which could let a remote malicious user cause a denial of service by sending the POST request to apply_cgi via the lang action without a language key. **CVE ID : CVE-2021-28845**	N/A	O-TRE-TEW--180821/684
vizio					
e50x-e1_firmware					
N/A	03-Aug-21	7.2	Vizio P65-F1 6.0.31.4-2 and E50x-E1 10.0.31.4-2 Smart TVs allow a threat actor to execute arbitrary code from a USB drive via the Smart Cast functionality, because files on the USB drive are effectively under the web root and can be executed.	N/A	O-VIZ-E50X-180821/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27942		
Improper Restriction of Excessive Authentication Attempts	02-Aug-21	5	The pairing procedure used by the Vizio P65-F1 6.0.31.4-2 and E50x-E1 10.0.31.4-2 Smart TVs and mobile application is vulnerable to a brute-force attack (against only 10000 possibilities), allowing a threat actor to forcefully pair the device, leading to remote control of the TV settings and configurations. **CVE ID : CVE-2021-27943**	https://www.vizio.com	O-VIZ-E50X-180821/686
p65-f1_firmware					
N/A	03-Aug-21	7.2	Vizio P65-F1 6.0.31.4-2 and E50x-E1 10.0.31.4-2 Smart TVs allow a threat actor to execute arbitrary code from a USB drive via the Smart Cast functionality, because files on the USB drive are effectively under the web root and can be executed. **CVE ID : CVE-2021-27942**	N/A	O-VIZ-P65--180821/687
Improper Restriction of Excessive Authentication Attempts	02-Aug-21	5	The pairing procedure used by the Vizio P65-F1 6.0.31.4-2 and E50x-E1 10.0.31.4-2 Smart TVs and mobile application is vulnerable to a brute-force attack (against only 10000 possibilities), allowing a threat actor to forcefully pair the device, leading to remote control of the TV settings and configurations.	https://www.vizio.com	O-VIZ-P65--180821/688

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-2021-27943		
ZTE					
zxctn_6120h_firmware					
Insufficient Verification of Data Authenticity	05-Aug-21	2.1	A ZTE's product of the transport network access layer has a security vulnerability. Because the system does not sufficiently verify the data reliability, attackers could replace an authenticated optical module on the equipment with an unauthenticated one, bypassing system authentication and detection, thus affecting signal transmission. This affects: <ZXCTN 6120H><V5.10.00B24> **CVE ID : CVE-2021-21739**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1017024	O-ZTE-ZXCT-180821/689
zxiptv_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-21	4.3	ZTE's big video business platform has two reflective cross-site scripting (XSS) vulnerabilities. Due to insufficient input verification, the attacker could implement XSS attacks by tampering with the parameters, to affect the operations of valid users. This affects: <ZXIPTV><ZXIPTV-EAS_PV5.06.04.09> **CVE ID : CVE-2021-21738**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1016764	O-ZTE-ZXIP-180821/690