National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 - 30 Jun 2022 Vol. 09 No. 12

Table of Content

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 74cms					
Product: 74cmsse					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the component /index/jobfairol/show/. **CVE ID : CVE-2022-32124**	N/A	A-74C-74CM-060722/1
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /job. **CVE ID : CVE-2022-32125**	N/A	A-74C-74CM-060722/2
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /company. **CVE ID : CVE-2022-32126**	N/A	A-74C-74CM-060722/3
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /company/view_be_browsed/total.	N/A	A-74C-74CM-060722/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32127		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /company/service/increment/add/im. **CVE ID : CVE-2022-32128**	N/A	A-74C-74CM-060722/5
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /company/account/safety/trade. **CVE ID : CVE-2022-32129**	N/A	A-74C-74CM-060722/6
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /company/down_resume/total/nature. **CVE ID : CVE-2022-32130**	N/A	A-74C-74CM-060722/7
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	74cmsSE v3.5.1 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the path /index/notice/show. **CVE ID : CVE-2022-32131**	N/A	A-74C-74CM-060722/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jun-22	7.5	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /home/job/index. **CVE ID : CVE-2022-33092**	N/A	A-74C-74CM-060722/9
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jun-22	7.5	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the key parameter at /freelance/resume_list. **CVE ID : CVE-2022-33093**	N/A	A-74C-74CM-060722/10
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jun-22	7.5	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /home/job/map. **CVE ID : CVE-2022-33094**	N/A	A-74C-74CM-060722/11
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jun-22	7.5	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /home/jobfairol/resumelist. **CVE ID : CVE-2022-33095**	N/A	A-74C-74CM-060722/12
Improper Neutralizat	23-Jun-22	7.5	74cmsSE v3.5.1 was discovered to contain	N/A	A-74C-74CM-060722/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			a SQL injection vulnerability via the keyword parameter at /home/resume/index . **CVE ID : CVE-2022-33096**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jun-22	7.5	74cmsSE v3.5.1 was discovered to contain a SQL injection vulnerability via the keyword parameter at /home/campus/campus_job. **CVE ID : CVE-2022-33097**	N/A	A-74C-74CM-060722/14
Vendor: Acquia					
Product: mautic					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-22	6.1	A cross-site scripting (XSS) vulnerability in the web tracking component of Mautic before 4.3.0 allows remote attackers to inject executable javascript **CVE ID : CVE-2022-25772**	N/A	A-ACQ-MAUT-060722/15
Vendor: adaware					
Product: protect					
Improper Privilege Management	16-Jun-22	7.8	Insecure permissions configuration in Adaware Protect v1.2.439.4251 allows attackers to escalate privileges via changing the service binary path.	N/A	A-ADA-PROT-060722/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31464		
Vendor: Adobe					
Product: animate					
Out-of-bounds Write	16-Jun-22	7.8	Adobe Animate version 22.0.5 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30664**	https://helpx.adobe.com/security/products/animate/apsb22-24.html	A-ADO-ANIM-060722/17
Product: incopy					
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30650**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	A-ADO-INCO-060722/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30651**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	A-ADO-INCO-060722/19
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30652**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	A-ADO-INCO-060722/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30653**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	A-ADO-INCO-060722/21
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30654**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	A-ADO-INCO-060722/22
Use After Free	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Use-After-Free	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	A-ADO-INCO-060722/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30655**		
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30656**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	A-ADO-INCO-060722/24
Use After Free	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	A-ADO-INCO-060722/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30657**		
Product: indesign					
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30658**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	A-ADO-INDE-060722/26
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	A-ADO-INDE-060722/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30659		
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30660**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	A-ADO-INDE-060722/28
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30661**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	A-ADO-INDE-060722/29
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1	https://helpx.adobe.com/security/products/i	A-ADO-INDE-060722/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30662**	ndesign/apsb22-30.html	
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30663**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	A-ADO-INDE-060722/31
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	A-ADO-INDE-060722/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30665**		
Product: robohelp_server					
Improper Authorization	16-Jun-22	8.8	RoboHelp Server earlier versions than RHS 11 Update 3 are affected by an Improper Authorization vulnerability which could lead to privilege escalation. An authenticated attacker could leverage this vulnerability to achieve full administrator privileges. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2022-30670**	https://helpx.adobe.com/security/products/robohelp-server/apsb22-31.html	A-ADO-ROBO-060722/33
Vendor: allow_svg_files_project					
Product: allow_svg_files					
Unrestricted Upload of File with Dangerous Type	20-Jun-22	7.2	The Allow svg files WordPress plugin before 1.1 does not properly validate uploaded files, which could allow high privilege users such as admin to upload PHP files even when	N/A	A-ALL-ALLO-060722/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they are not allowed to **CVE ID : CVE-2022-1939**		
Vendor: amazon_einzeltitellinks_project					
Product: amazon_einzeltitellinks					
Cross-Site Request Forgery (CSRF)	20-Jun-22	6.5	The Amazon Einzeltitellinks WordPress plugin through 1.3.3 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping **CVE ID : CVE-2022-1830**	N/A	A-AMA-AMAZ-060722/35
Vendor: angtech					
Product: haraj					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-22	5.4	A cross-site scripting vulnerability in the ads comment section of Haraj v3.7 allows attackers to execute arbitrary web scripts or HTML via a crafted POST request. **CVE ID : CVE-2022-31298**	https://angtech.org, https://angtech.org/product/view/3	A-ANG-HARA-060722/36
Improper Neutralization of Input During	16-Jun-22	6.1	Haraj v3.7 was discovered to contain a reflected cross-site scripting (XSS)	N/A	A-ANG-HARA-060722/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			vulnerability in the User Upgrade Form. **CVE ID : CVE-2022-31299**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-22	5.4	A cross-site scripting vulnerability in the DM Section component of Haraj v3.7 allows attackers to execute arbitrary web scripts or HTML via a crafted POST request. **CVE ID : CVE-2022-31300**	https://angtech.org, https://angtech.org/product/view/3	A-ANG-HARA-060722/38
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-22	5.4	Haraj v3.7 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the Post Ads component. **CVE ID : CVE-2022-31301**	https://angtech.org, https://angtech.org/product/view/3	A-ANG-HARA-060722/39
Vendor: Apache					
Product: sling_api					
Improper Encoding or Escaping of Output	22-Jun-22	5.3	Apache Sling Commons Log <= 5.4.0 and Apache Sling API <= 2.25.0 are vulnerable to log injection. The ability to forge logs may allow an attacker to cover tracks by injecting fake logs and potentially corrupt log files. **CVE ID : CVE-2022-32549**	https://lists.apache.org/thread/7z6h3806mwcov5kx6l96pq839sn0po1v	A-APA-SLIN-060722/40
Product: sling_commons_log					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	22-Jun-22	5.3	Apache Sling Commons Log <= 5.4.0 and Apache Sling API <= 2.25.0 are vulnerable to log injection. The ability to forge logs may allow an attacker to cover tracks by injecting fake logs and potentially corrupt log files. **CVE ID : CVE-2022-32549**	https://lists.apache.org/thread/7z6h3806mwcov5kx6l96pq839sn0po1v	A-APA-SLIN-060722/41
Product: tomcat					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability. **CVE ID : CVE-2022-34305**	https://lists.apache.org/thread/k04zk0nq6w57m72w5gb0r6z9ryhmvr4k	A-APA-TOMC-060722/42
Vendor: argo_events_project					
Product: argo_events					
Improper Limitation of a Pathname to a Restricted Directory	17-Jun-22	7.5	The package github.com/argoproj/argo-events/sensors/artifacts before 1.7.1 are vulnerable to Directory Traversal in the (g *GitArtifactReader).R	https://snyk.io/vuln/SNYK-GOLANG-GITHUBCOMARGOPROJARGOEVENTSSENSORSARTIFACTS-2864522, https://github.	A-ARG-ARGO-060722/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			ead() API in git.go. This could allow arbitrary file reads if the GitArtifactReader is provided a pathname containing a symbolic link or an implicit directory name such as ... **CVE ID : CVE-2022-25856**	com/argoproj/argo-events/commit/d0f66dbce78bc31923ca057b20fc722aa24ca961, https://github.com/argoproj/argo-events/issues/1947	
Vendor: Artifex					
Product: ghostscript					
NULL Pointer Dereference	16-Jun-22	5.5	A NULL pointer dereference vulnerability was found in Ghostscript, which occurs when it tries to render a large number of bits in memory. When allocating a buffer device, it relies on an init_device_procs defined for the device that uses it as a prototype that depends upon the number of bits per pixel. For bpp > 64, mem_x_device is used and does not have an init_device_procs defined. This flaw allows an attacker to parse a large number of bits (more than 64 bits per pixel), which triggers a NULL pointer dereference flaw, causing an application to crash.	https://bugs.ghostscript.com/show_bug.cgi?id=704945, http://git.ghostscript.com/?p=ghostpdl.git;h=ae1061d948d88667bdf51d47d918c4684d0f67df, https://bugzilla.redhat.com/show_bug.cgi?id=2095261	A-ART-GHOS-060722/44

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2085		
Vendor: Asus					
Product: control_center					
Incorrect Authorization	20-Jun-22	6.5	ASUS Control Center API has a broken access control vulnerability. An unauthenticated remote attacker can call privileged API functions to perform partial system operations or cause partial disrupt of service. **CVE ID : CVE-2022-26668**	N/A	A-ASU-CONT-060722/45
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jun-22	6.5	ASUS Control Center is vulnerable to SQL injection. An authenticated remote attacker with general user privilege can inject SQL command to specific API parameters to acquire database schema or access data. **CVE ID : CVE-2022-26669**	N/A	A-ASU-CONT-060722/46
Vendor: atlasvpn					
Product: atlasvpn					
Improper Privilege Management	21-Jun-22	8.8	AtlasVPN - Privilege Escalation Lack of proper security controls on named pipe messages can allow an attacker with low privileges to send a malicious	N/A	A-ATL-ATLA-060722/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload and gain SYSTEM permissions on a windows computer where the AtlasVPN client is installed. **CVE ID : CVE-2022-23171**		
Vendor: Autodesk					
Product: 3ds_max					
Out-of-bounds Read	16-Jun-22	7.8	A maliciously crafted TIF file can be forced to read beyond allocated boundaries in Autodesk 3ds Max 2022, and 2021 when parsing the TIF files. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-27531**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0010	A-AUT-3DS_-060722/48
Out-of-bounds Write	16-Jun-22	7.8	A maliciously crafted TIF file in Autodesk 3ds Max 2022 and 2021 can be used to write beyond the allocated buffer while parsing TIF files. This vulnerability in conjunction with other vulnerabilities could lead to arbitrary code execution. **CVE ID : CVE-2022-27532**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0010	A-AUT-3DS_-060722/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-3DS_-060722/50
Product: advance_steel					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-ADVA-060722/51
Product: autocad					
Use After Free	21-Jun-22	7.8	A maliciously crafted JT file in Autodesk AutoCAD 2022, 2021, 2020, 2019 can be used to trigger use-after-free vulnerability. Exploitation of this vulnerability may	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0002	A-AUT-AUTO-060722/52

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to code execution. **CVE ID : CVE-2022-27867**		
Use After Free	21-Jun-22	7.8	A maliciously crafted CAT file in Autodesk AutoCAD 2023 can be used to trigger use-after-free vulnerability. Exploitation of this vulnerability may lead to code execution. **CVE ID : CVE-2022-27868**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0005	A-AUT-AUTO-060722/53
Out-of-bounds Read	21-Jun-22	7.8	A maliciously crafted TIFF file in Autodesk AutoCAD 2023 can be forced to read and write beyond allocated boundaries when parsing the TIFF file. This vulnerability can be exploited to execute arbitrary code. **CVE ID : CVE-2022-27869**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-060722/54
Out-of-bounds Write	21-Jun-22	7.8	A maliciously crafted TGA file in Autodesk AutoCAD 2023 may be used to write beyond the allocated buffer while parsing TGA file. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27870**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0004	A-AUT-AUTO-060722/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-AUTO-060722/56
Product: autocad_architecture					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-AUTO-060722/57
Product: autocad_civil_3d					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-AUTO-060722/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**		
Product: autocad_electrical					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-AUTO-060722/59
Product: autocad_lt					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-AUTO-060722/60
Product: autocad_map_3d					
Allocation of Resources	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and	https://www.autodesk.com/trust/security-	A-AUT-AUTO-060722/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**	advisories/adsk-sa-2022-0011	
Product: autocad_mechanical					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-AUTO-060722/62
Product: autocad_mep					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-AUTO-060722/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27871		
Product: autocad_plant_3d					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-AUTO-060722/64
Product: design_review					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-DESI-060722/65
Product: navisworks					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-NAVI-060722/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used to write beyond the allocated buffer while parsing PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**		
Improper Handling of Exceptional Conditions	21-Jun-22	7.8	A maliciously crafted PDF file may be used to dereference a pointer for read or write operation while parsing PDF files in Autodesk Navisworks 2022. The vulnerability exists because the application fails to handle a crafted PDF file, which causes an unhandled exception. An attacker can leverage this vulnerability to cause a crash or read sensitive data or execute arbitrary code. **CVE ID : CVE-2022-27872**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-NAVI-060722/67
Product: revit					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.8	Autodesk AutoCAD product suite, Revit, Design Review and Navisworks releases using PDFTron prior to 9.1.17 version may be used to write beyond the allocated buffer while parsing	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0011	A-AUT-REVI-060722/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PDF files. This vulnerability may be exploited to execute arbitrary code. **CVE ID : CVE-2022-27871**		
Vendor: Blynk					
Product: blynk-library					
Out-of-bounds Write	17-Jun-22	9.8	A stack-based buffer overflow vulnerability exists in the BlynkConsole.h runCommand functionality of Blynk -Library v1.0.1. A specially-crafted network request can lead to command execution. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-29496**	N/A	A-BLY-BLYN-060722/69
Vendor: Broadcom					
Product: ca_automic_automation					
Improper Authentication	16-Jun-22	9.8	CA Automic Automation 12.2 and 12.3 contain an authentication error vulnerability in the Automic agent that could allow a remote attacker to potentially execute arbitrary commands. **CVE ID : CVE-2022-33750**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/20629	A-BRO-CA_A-060722/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	16-Jun-22	7.5	CA Automic Automation 12.2 and 12.3 contain an insecure memory handling vulnerability in the Automic agent that could allow a remote attacker to potentially access sensitive data. **CVE ID : CVE-2022-33751**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/20629	A-BRO-CA_A-060722/71
Improper Input Validation	16-Jun-22	9.8	CA Automic Automation 12.2 and 12.3 contain an insufficient input validation vulnerability in the Automic agent that could allow a remote attacker to potentially execute arbitrary code. **CVE ID : CVE-2022-33752**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/20629	A-BRO-CA_A-060722/72
Exposure of Resource to Wrong Sphere	16-Jun-22	8.8	CA Automic Automation 12.2 and 12.3 contain an insecure file creation and handling vulnerability in the Automic agent that could allow a user to potentially elevate privileges. **CVE ID : CVE-2022-33753**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/20629	A-BRO-CA_A-060722/73
Improper Input Validation	16-Jun-22	9.8	CA Automic Automation 12.2 and 12.3 contain an insufficient input validation	https://support.broadcom.com/web/ecx/support-content-notification/-	A-BRO-CA_A-060722/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the Automic agent that could allow a remote attacker to potentially execute arbitrary code. **CVE ID : CVE-2022-33754**	/external/content/SecurityAdvisories/0/20629	
Improper Input Validation	16-Jun-22	5.3	CA Automic Automation 12.2 and 12.3 contain an insecure input handling vulnerability in the Automic Agent that could allow a remote attacker to potentially enumerate users. **CVE ID : CVE-2022-33755**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/20629	A-BRO-CA_A-060722/75
Insufficient Entropy	16-Jun-22	7.5	CA Automic Automation 12.2 and 12.3 contain an entropy weakness vulnerability in the Automic AutomationEngine that could allow a remote attacker to potentially access sensitive data. **CVE ID : CVE-2022-33756**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/20629	A-BRO-CA_A-060722/76
Product: ca_clarity					
XML Injection (aka Blind XPath Injection)	16-Jun-22	7.5	CA Clarity 15.8 and below and 15.9.0 contain an insecure XML parsing vulnerability that could allow a remote attacker to potentially	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAd	A-BRO-CA_C-060722/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			view the contents of any file on the system. **CVE ID : CVE-2022-33739**	visories/0/20645	
Vendor: capa_protect_project					
Product: capa_protect					
Cross-Site Request Forgery (CSRF)	20-Jun-22	6.5	The CaPa Protect WordPress plugin through 0.5.8.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and disable the applied protection. **CVE ID : CVE-2022-1832**	N/A	A-CAP-CAPA-060722/78
Vendor: Cisco					
Product: adaptive_security_device_manager					
Insertion of Sensitive Information into Log File	22-Jun-22	5.5	A vulnerability in the logging component of Cisco Adaptive Security Device Manager (ASDM) could allow an authenticated, local attacker to view sensitive information in clear text on an affected system. Cisco ADSM must be deployed in a shared workstation environment for this issue to be exploited. This vulnerability is due to the storage of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-logging-jnLOY422	A-CIS-ADAP-060722/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unencrypted credentials in certain logs. An attacker could exploit this vulnerability by accessing the logs on an affected system. A successful exploit could allow the attacker to view the credentials of other users of the shared device. **CVE ID : CVE-2022-20651**		
Vendor: Citrix					
Product: application_delivery_management					
Incorrect Authorization	16-Jun-22	8.1	Corruption of the system by a remote, unauthenticated user. The impact of this can include the reset of the administrator password at the next device reboot, allowing an attacker with ssh access to connect with the default administrator credentials after the device has rebooted. **CVE ID : CVE-2022-27511**	https://support.citrix.com/article/CTX460016/citrix-application-delivery-management-security-bulletin-for-cve202227511-and-cve202227512	A-CIT-APPL-060722/80
Use After Free	16-Jun-22	5.3	Temporary disruption of the ADM license service. The impact of this includes preventing new licenses from being issued or renewed by Citrix ADM.	https://support.citrix.com/article/CTX460016/citrix-application-delivery-management-security-bulletin-for-	A-CIT-APPL-060722/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27512	cve202227511-and-cve202227512	
Vendor: colorlib					
Product: coming_soon_\&_maintenance_mode					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-22	4.8	The Coming Soon & Maintenance Mode by Colorlib WordPress plugin before 1.0.99 does not sanitize and escape some settings, allowing high privilege users such as admin to perform Stored Cross-Site Scripting when unfiltered_html is disallowed (for example in multisite setup) **CVE ID : CVE-2022-1945**	N/A	A-COL-COMI-060722/82
Vendor: Comodo					
Product: antivirus					
Improper Privilege Management	21-Jun-22	7.8	Comodo Antivirus 12.2.2.8012 has a quarantine flaw that allows privilege escalation. To escalate privilege, a low-privileged attacker can use an NTFS directory junction to restore a malicious DLL from quarantine into the System32 folder. **CVE ID : CVE-2022-34008**	https://antivirus.comodo.com/	A-COM-ANTI-060722/83
Vendor: cross-linker_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cross-linker					
Cross-Site Request Forgery (CSRF)	20-Jun-22	6.5	The Cross-Linker WordPress plugin through 3.0.1.9 does not have CSRF check in place when creating Cross-Links, which could allow attackers to make a logged in admin perform such action via a CSRF attack **CVE ID : CVE-2022-1826**	N/A	A-CRO-CROS-060722/84
Vendor: devolutions					
Product: remote_desktop_manager					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Jun-22	7.5	A path traversal issue in entry attachments in Devolutions Remote Desktop Manager before 2022.2 allows attackers to create or overwrite files in an arbitrary location. **CVE ID : CVE-2022-33995**	N/A	A-DEV-REMO-060722/85
Vendor: diffy_project					
Product: diffy					
N/A	23-Jun-22	9.8	The function that calls the diff tool in Diffy 3.4.1 does not properly handle double quotes in a filename when run in a windows environment. This allows attackers to execute arbitrary commands via a crafted string.	https://github.com/samg/diffy/commit/478f392082b66d38f54a02b4bb9c41be32fd6593	A-DIF-DIFF-060722/86

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33127		
Vendor: directory_management_system_project					
Product: directory_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jun-22	9.8	Directory Management System v1.0 was discovered to contain a SQL injection vulnerability via the searchdata parameter in search-dirctory.php. **CVE ID : CVE-2022-31382**	N/A	A-DIR-DIRE-060722/87
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jun-22	9.8	Directory Management System v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter in view-directory.php. **CVE ID : CVE-2022-31383**	N/A	A-DIR-DIRE-060722/88
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jun-22	9.8	Directory Management System v1.0 was discovered to contain a SQL injection vulnerability via the fullname parameter in add-directory.php. **CVE ID : CVE-2022-31384**	N/A	A-DIR-DIRE-060722/89
Vendor: discordjs					
Product: opus					
Use of Uninitialized Resource	17-Jun-22	7.5	All versions of package @discordjs/opus are vulnerable to Denial	https://snyk.io/vuln/SNYK-JS-DISCORDJSOP	A-DIS-OPUS-060722/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS) when trying to encode using an encoder with zero channels, or a non-initialized buffer. This leads to a hard crash. **CVE ID : CVE-2022-25345**	US-2403100, https://github.com/discordjs/opus/blob/3ca4341ffdd81cf83cec57045e59e228e6017590/src/node-opus.cc%23L28	
Vendor: discourse					
Product: discourse-chat					
Exposure of Sensitive Information to an Unauthorized Actor	21-Jun-22	6.5	discourse-chat is a chat plugin for the Discourse application. Versions prior to 0.4 are vulnerable to an exposure of sensitive information, where an attacker who knows the message ID for a channel they do not have access to can view that message using the chat message lookup endpoint, primarily affecting direct message channels. There are no known workarounds for this issue, and users are advised to update the plugin. **CVE ID : CVE-2022-31095**	https://github.com/discourse/discourse-chat/security/advisories/GHSA-r979-jhp2-3f6h	A-DIS-DISC-060722/91
Vendor: e-dynamics					
Product: events_made_easy					
Improper Neutralization of Special	20-Jun-22	9.8	The Events Made Easy WordPress plugin before 2.2.81 does not properly	N/A	A-E-D-EVEN-060722/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection **CVE ID : CVE-2022-1905**		
Vendor: electrum					
Product: electrum					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	17-Jun-22	5.5	paymentrequest.py in Electrum before 4.2.2 allows a file:// URL in the r parameter of a payment request (e.g., within QR code data). On Windows, this can lead to capture of credentials over SMB. On Linux and UNIX, it can lead to a denial of service by specifying the /dev/zero filename. **CVE ID : CVE-2022-31246**	N/A	A-ELE-ELEC-060722/93
Vendor: F5					
Product: nginx					
Use After Free	21-Jun-22	5.5	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_string_offset at src/njs_string.c. **CVE ID : CVE-2022-31307**	https://github.com/nginx/njs/commit/eafe4c7a326b163612f10861392622b5da5b1792	A-F5-NGIN-060722/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	21-Jun-22	5.5	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_vmcode_interpreter at src/njs_vmcode.c. **CVE ID : CVE-2022-32414**	https://github.com/nginx/njs/commit/31ed93a5623f24ca94e6d47e895ba735d9d97d46	A-F5-NGIN-060722/95
Product: njs					
Use After Free	21-Jun-22	5.5	Nginx NJS v0.7.2 was discovered to contain a segmentation violation in the function njs_array_convert_to_slow_array at src/njs_array.c. **CVE ID : CVE-2022-31306**	https://github.com/nginx/njs/commit/81af26364c21c196dd21fb5e14c7fa9ce7debd17	A-F5-NJS-060722/96
Vendor: fast_string_search_project					
Product: fast_string_search					
Incorrect Calculation	17-Jun-22	7.5	All versions of package fast-string-search are vulnerable to Denial of Service (DoS) when computations are incorrect for non-string inputs. One can cause the V8 to attempt reading from non-permitted locations and cause a segmentation fault due to the violation. **CVE ID : CVE-2022-22138**	https://snyk.io/vuln/SNYK-JS-FASTSTRINGSEARCH-2392367	A-FAS-FAST-060722/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	17-Jun-22	5.3	All versions of package fast-string-search are vulnerable to Out-of-bounds Read due to incorrect memory freeing and length calculation for any non-string input as the source. This allows the attacker to read previously allocated memory. **CVE ID : CVE-2022-25872**	https://snyk.io/vuln/SNYK-JS-FASTSTRINGSEARCH-2392368, https://github.com/magiclen/node-fast-string-search/blob/c8dd9fc966abc80b327f509e63360f59e0de9fb5/src/fast-string-search.c%23L192	A-FAS-FAST-060722/98
Vendor: fujielectric					
Product: monitouch_v-sft					
Out-of-bounds Write	16-Jun-22	7.8	Out-of-bounds write vulnerability exists in the simulator module contained in the graphic editor 'V-SFT' versions prior to v6.1.6.0, which may allow an attacker to obtain information and/or execute arbitrary code by having a user to open a specially crafted image file. **CVE ID : CVE-2022-30538**	https://monitouch.fujielectric.com/site/download-e/09vsft6_inf/Search.php	A-FUJ-MONI-060722/99
Out-of-bounds Read	16-Jun-22	7.8	Out-of-bounds read vulnerability exists in the simulator module contained in the graphic editor 'V-SFT' versions prior to	https://monitouch.fujielectric.com/site/download-e/09vsft6_inf/Search.php	A-FUJ-MONI-060722/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v6.1.6.0, which may allow an attacker to obtain information and/or execute arbitrary code by having a user to open a specially crafted image file. **CVE ID : CVE-2022-30546**		
Product: v-server					
Out-of-bounds Read	16-Jun-22	7.8	Out-of-bounds read vulnerability exists in V-Server v4.0.11.0 and earlier and V-Server Lite v4.0.13.0 and earlier, which may allow an attacker to obtain information and/or execute arbitrary code by having a user to open a specially crafted image file. **CVE ID : CVE-2022-30549**	https://monitouch.fujielectric.com/site/download-e/09vsft6_inf/Search.php, https://monitouch.fujielectric.com/site/download-eu/03tellus_inf/index.php	A-FUJ-V-SE-060722/101
Vendor: genivi					
Product: diagnostic_log_and_trace					
Double Free	16-Jun-22	7.5	An issue in dlt_config_file_parser.c of dlt-daemon v2.18.8 allows attackers to cause a double free via crafted TCP packets. **CVE ID : CVE-2022-31291**	https://github.com/COVESA/dlt-daemon/pull/376/commits	A-GEN-DIAG-060722/102
Vendor: getmotoradmin					
Product: motor_admin					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	22-Jun-22	8.8	In motor-admin versions 0.0.1 through 0.2.56 are vulnerable to host header injection in the password reset functionality where malicious actor can send fake password reset email to arbitrary victim. **CVE ID : CVE-2022-23079**	https://github.com/motor-admin/motor-admin/commit/a461b7507940a1fa062836daa89c82404fe3ecf9	A-GET-MOTO-060722/103
Vendor: Glpi-project					
Product: glpi_inventory					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Jun-22	5.3	### Impact A plugin public script can be used to read content of system files. ### Patches Upgrade to version 1.0.2. ### Workarounds `b/deploy/index.php` file can be deleted if deploy feature is not used. **CVE ID : CVE-2022-31062**	https://github.com/glpi-project/glpi-inventory-plugin/security/advisories/GHSA-q33f-jcjf-p4v9	A-GLP-GLPI-060722/104
Vendor: GNU					
Product: libredwg					
Reachable Assertion	23-Jun-22	7.5	There is an Assertion `int decode_preR13_entities(BITCODE_RL, BITCODE_RL, unsigned int, BITCODE_RL, BITCODE_RL, Bit_Chain *, Dwg_Data *' failed at dwg2dxf: decode.c:5801 in	N/A	A-GNU-LIBR-060722/105

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			libredwg v0.12.4.4608. **CVE ID : CVE-2022-33024**		
Use After Free	23-Jun-22	7.8	LibreDWG v0.12.4.4608 was discovered to contain a heap-use-after-free via the function decode_preR13_section at decode_r11.c. **CVE ID : CVE-2022-33025**	N/A	A-GNU-LIBR-060722/106
Out-of-bounds Write	23-Jun-22	7.8	LibreDWG v0.12.4.4608 was discovered to contain a heap buffer overflow via the function bit_calc_CRC at bits.c. **CVE ID : CVE-2022-33026**	N/A	A-GNU-LIBR-060722/107
Use After Free	23-Jun-22	7.8	LibreDWG v0.12.4.4608 was discovered to contain a heap-use-after-free via the function dwg_add_handleref at dwg.c. **CVE ID : CVE-2022-33027**	N/A	A-GNU-LIBR-060722/108
Out-of-bounds Write	23-Jun-22	7.8	LibreDWG v0.12.4.4608 was discovered to contain a heap buffer overflow via the function dwg_add_object at decode.c. **CVE ID : CVE-2022-33028**	N/A	A-GNU-LIBR-060722/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Jun-22	7.8	LibreDWG v0.12.4.4608 was discovered to contain a heap-buffer-overflow via the function decode_preR13_section_hdr at decode_r11.c. **CVE ID : CVE-2022-33032**	N/A	A-GNU-LIBR-060722/110
Double Free	23-Jun-22	7.8	LibreDWG v0.12.4.4608 was discovered to contain a double-free via the function dwg_read_file at dwg.c. **CVE ID : CVE-2022-33033**	N/A	A-GNU-LIBR-060722/111
Out-of-bounds Write	23-Jun-22	7.8	LibreDWG v0.12.4.4608 was discovered to contain a stack overflow via the function copy_bytes at decode_r2007.c. **CVE ID : CVE-2022-33034**	N/A	A-GNU-LIBR-060722/112
Vendor: got_project					
Product: got					
N/A	18-Jun-22	5.3	The got package before 12.1.0 (also fixed in 11.8.5) for Node.js allows a redirect to a UNIX socket. **CVE ID : CVE-2022-33987**	https://github.com/sindresorhus/got/pull/2047, https://github.com/sindresorhus/got/compare/v12.0.3...v12.1.0, https://github.	A-GOT-GOT-060722/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				com/sindresorhus/got/releases/tag/v11.8.5	
Vendor: grafana					
Product: grafana					
Improper Authentication	17-Jun-22	7.5	** DISPUTED ** Grafana 8.4.3 allows unauthenticated access via (for example) a /dashboard/snapshot/*?orgId=0 URI. NOTE: the vendor considers this a UI bug, not a vulnerability. **CVE ID : CVE-2022-32276**	N/A	A-GRA-GRAF-060722/114
Vendor: habitica					
Product: habitica					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-22	6.1	In habitica versions v4.119.0 through v4.232.2 are vulnerable to DOM XSS via the login page. **CVE ID : CVE-2022-23077**	https://github.com/HabitRPG/habitica/commit/5bcfdbe066e8c899f3ecf3fdcdbacc2ecba7f02f	A-HAB-HABI-060722/115
URL Redirection to Untrusted Site ('Open Redirect')	22-Jun-22	6.1	In habitica versions v4.119.0 through v4.232.2 are vulnerable to open redirect via the login page. **CVE ID : CVE-2022-23078**	https://github.com/HabitRPG/habitica/commit/5bcfdbe066e8c899f3ecf3fdcdbacc2ecba7f02f	A-HAB-HABI-060722/116
Vendor: hyland					
Product: onbase					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Jun-22	5.3	The Hyland Onbase Application Server releases prior to 20.3.58.1000 and OnBase releases 21.1.1.1000 through 21.1.15.1000 are vulnerable to a username enumeration vulnerability. An attacker can obtain valid users based on the response returned for invalid and valid users by sending a POST login request to the /mobilebroker/ServiceToBroker.svc/Json/Connect endpoint. This can lead to user enumeration against the underlying Active Directory integrated systems. **CVE ID : CVE-2022-23342**	https://community.hyland.com/login?returnUrl=/connect/hyland-research-and-development/security-advisories/username-enumeration-in-onbase	A-HYL-ONBA-060722/117
Vendor: IBM					
Product: curam_social_program_management					
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 218281.	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218281	A-IBM-CURA-060722/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22317		
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. **CVE ID : CVE-2022-22318**	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218283	A-IBM-CURA-060722/119
Product: robotic_process_automation					
Exposure of Resource to Wrong Sphere	20-Jun-22	5.5	IBM Robotic Process Automation 21.0.2 could allow a local user to obtain sensitive web service configuration credentials from system memory. IBM X-Force ID: 223026. **CVE ID : CVE-2022-22414**	https://exchange.xforce.ibmcloud.com/vulnerabilities/223026, https://www.ibm.com/support/pages/node/6596071	A-IBM-ROBO-060722/120
Exposure of Resource to Wrong Sphere	17-Jun-22	6.5	IBM Robotic Process Automation 20.10.0, 20.12.5, 21.0.0, 21.0.1, and 21.0.2 contains a vulnerability that could allow a user to obtain sensitive information due to information properly masked in the control center UI. IBM X-Force ID: 227294. **CVE ID : CVE-2022-30607**	https://www.ibm.com/support/pages/node/6595759, https://exchange.xforce.ibmcloud.com/vulnerabilities/227294	A-IBM-ROBO-060722/121
Product: spectrum_protect_operations_center					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	17-Jun-22	9.8	In some cases, an unsuccessful attempt to log into IBM Spectrum Protect Operations Center 8.1.0.000 through 8.1.14.000 does not cause the administrator's invalid sign-on count to be incremented on the IBM Spectrum Protect Server. An attacker could exploit this vulnerability using brute force techniques to gain unauthorized administrative access to the IBM Spectrum Protect Server. IBM X-Force ID: 226325. **CVE ID : CVE-2022-22485**	https://exchange.xforce.ibmcloud.com/vulnerabilities/226325, https://www.ibm.com/support/pages/node/6595655	A-IBM-SPEC-060722/122
Vendor: ideaco					
Product: idealms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	6.1	IdeaLMS 2022 allows reflected Cross Site Scripting (XSS) via the IdeaLMS/Class/Assessment/ PATH_INFO. **CVE ID : CVE-2022-31786**	N/A	A-IDE-IDEA-060722/123
Product: ideatms					
Improper Neutralization of Special Elements used in an	23-Jun-22	9.8	IdeaTMS 2022 is vulnerable to SQL Injection via the PATH_INFO	N/A	A-IDE-IDEA-060722/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			**CVE ID : CVE-2022-31787**		
Vendor: infogami					
Product: infogami					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-22	5.4	In openlibrary versions deploy-2016-07-0 through deploy-2021-12-22 are vulnerable to Stored XSS. **CVE ID : CVE-2022-32159**	https://github.com/internetarchive/infogami/pull/195/commits/ccc2141c5fb093870c9e2742c01336ecca8cd12e	A-INF-INFO-060722/125
Vendor: inline_google_maps_project					
Product: inline_google_maps					
Cross-Site Request Forgery (CSRF)	20-Jun-22	6.5	The Inline Google Maps WordPress plugin through 5.11 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack, and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping **CVE ID : CVE-2022-1829**	N/A	A-INL-INLI-060722/126
Vendor: inventree					
Product: inventree					
Unrestricted Upload of File with	17-Jun-22	8.8	Unrestricted Upload of File with Dangerous Type in GitHub repository	https://github.com/inventree/inventree/commit/26bf51c	A-INV-INVE-060722/127

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			inventree/inventree prior to 0.7.2. **CVE ID : CVE-2022-2111**	20a1c9b3130ac5dd2e17649bece5ff84f, https://huntr.dev/bounties/a0e5c68e-0f75-499b-bd7b-d935fb8c0cd1	
Improper Neutralization of Formula Elements in a CSV File	17-Jun-22	8.8	Improper Neutralization of Formula Elements in a CSV File in GitHub repository inventree/inventree prior to 0.7.2. **CVE ID : CVE-2022-2112**	https://github.com/inventree/inventree/commit/26bf51c20a1c9b3130ac5dd2e17649bece5ff84f, https://huntr.dev/bounties/e57c36e7-fa39-435f-944a-3a52ee066f73	A-INV-INVE-060722/128
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jun-22	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository inventree/inventree prior to 0.7.2. **CVE ID : CVE-2022-2113**	https://github.com/inventree/inventree/commit/26bf51c20a1c9b3130ac5dd2e17649bece5ff84f, https://huntr.dev/bounties/4cae8442-c042-43c2-ad89-6f666eaf3d57	A-INV-INVE-060722/129
Vendor: inventree_project					
Product: inventree					
Uncontrolled Resource Consumption	20-Jun-22	6.5	Denial of Service in GitHub repository inventree/inventree prior to 0.8.0.	https://huntr.dev/bounties/57b0f272-a97f-4cb3-b546-	A-INV-INVE-060722/130

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2134	c863c68a561a, https://github.com/inventree/inventree/commit/63b4ff3eb6e80861962fafe79c9b483cd7239d6c	
Vendor: Iobit					
Product: iotransfer					
Improper Authentication	16-Jun-22	9.8	In IOBit IOTransfer 4.3.1.1561, an unauthenticated attacker can send GET and POST requests to Airserv and gain arbitrary read/write access to the entire file-system (with admin privileges) on the victim's endpoint, which can result in data theft and remote code execution. **CVE ID : CVE-2022-24562**	N/A	A-IOB-IOTR-060722/131
Vendor: ispyconnect					
Product: ispy					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Jun-22	9.8	iSpyConnect iSpy v7.2.2.0 is vulnerable to path traversal. **CVE ID : CVE-2022-29774**	N/A	A-ISP-ISPY-060722/132
Improper Authentication	21-Jun-22	9.8	iSpyConnect iSpy v7.2.2.0 allows attackers to bypass	N/A	A-ISP-ISPY-060722/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication via a crafted URL. **CVE ID : CVE-2022-29775**		
Vendor: Jenkins					
Product: agent_server_parameter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	5.4	Jenkins Agent Server Parameter Plugin 1.1 and earlier does not escape the name and description of Agent Server parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. **CVE ID : CVE-2022-34183**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2784	A-JEN-AGEN-060722/134
Product: beaker_builder					
Cross-Site Request Forgery (CSRF)	23-Jun-22	6.5	A cross-site request forgery (CSRF) vulnerability in Jenkins Beaker builder Plugin 1.10 and earlier allows attackers to connect to an attacker-specified URL. **CVE ID : CVE-2022-34207**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2248	A-JEN-BEAK-060722/135
Missing Authorization	23-Jun-22	4.3	A missing permission check in Jenkins Beaker builder Plugin 1.10 and earlier allows attackers with Overall/Read	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2248	A-JEN-BEAK-060722/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission to connect to an attacker-specified URL. **CVE ID : CVE-2022-34208**		
Product: convertigo_mobile_platform					
Unprotected Storage of Credentials	23-Jun-22	6.5	Jenkins Convertigo Mobile Platform Plugin 1.1 and earlier stores passwords unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission, or access to the Jenkins controller file system. **CVE ID : CVE-2022-34199**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2064	A-JEN-CONV-060722/137
Cross-Site Request Forgery (CSRF)	23-Jun-22	6.5	A cross-site request forgery (CSRF) vulnerability in Jenkins Convertigo Mobile Platform Plugin 1.1 and earlier allows attackers to connect to an attacker-specified URL. **CVE ID : CVE-2022-34200**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2276	A-JEN-CONV-060722/138
Missing Authorization	23-Jun-22	6.5	A missing permission check in Jenkins Convertigo Mobile Platform Plugin 1.1 and earlier allows attackers with Overall/Read permission to connect	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2276	A-JEN-CONV-060722/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to an attacker-specified URL. **CVE ID : CVE-2022-34201**		
Product: easyqa					
Unprotected Storage of Credentials	23-Jun-22	6.5	Jenkins EasyQA Plugin 1.0 and earlier stores user passwords unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system. **CVE ID : CVE-2022-34202**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2066	A-JEN-EASY-060722/140
Cross-Site Request Forgery (CSRF)	23-Jun-22	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins EasyQA Plugin 1.0 and earlier allows attackers to connect to an attacker-specified HTTP server. **CVE ID : CVE-2022-34203**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2281	A-JEN-EASY-060722/141
Missing Authorization	23-Jun-22	4.3	A missing permission check in Jenkins EasyQA Plugin 1.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified HTTP server.	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2281	A-JEN-EASY-060722/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34204		
Product: embeddable_build_status					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	Jenkins Embeddable Build Status Plugin 2.0.3 allows specifying a 'link' query parameter that build status badges will link to, without restricting possible values, resulting in a reflected cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2022-34178**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2567	A-JEN-EMBE-060722/143
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jun-22	7.5	Jenkins Embeddable Build Status Plugin 2.0.3 and earlier allows specifying a \`style\` query parameter that is used to choose a different SVG image style without restricting possible values, resulting in a relative path traversal vulnerability that allows attackers without Overall/Read permission to specify paths to other SVG images on the Jenkins controller file system. **CVE ID : CVE-2022-34179**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2792	A-JEN-EMBE-060722/144
Missing Authorization	23-Jun-22	7.5	Jenkins Embeddable Build Status Plugin 2.0.3 and earlier does not correctly perform	https://www.jenkins.io/security/advisory/2022-06-	A-JEN-EMBE-060722/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the ViewStatus permission check in the HTTP endpoint it provides for "unprotected" status badge access, allowing attackers without any permissions to obtain the build status badge icon for any attacker-specified job and/or build. **CVE ID : CVE-2022-34180**	22/#SECURITY-2794	
Product: jenkins					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	In Jenkins 2.320 through 2.355 (both inclusive) and LTS 2.332.1 through LTS 2.332.3 (both inclusive) the help icon does not escape the feature name that is part of its tooltip, effectively undoing the fix for SECURITY-1955, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission. **CVE ID : CVE-2022-34170**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2781	A-JEN-JENK-060722/146
Improper Neutralization of Input During Web Page	23-Jun-22	6.1	In Jenkins 2.321 through 2.355 (both inclusive) and LTS 2.332.1 through LTS 2.332.3 (both inclusive) the HTML	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2781	A-JEN-JENK-060722/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			output generated for new symbol-based SVG icons includes the 'title' attribute of 'l:ionicon' (until Jenkins 2.334) and 'alt' attribute of 'l:icon' (since Jenkins 2.335) without further escaping, resulting in a cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2022-34171**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	In Jenkins 2.340 through 2.355 (both inclusive) symbol-based icons unescape previously escaped values of 'tooltip' parameters, resulting in a cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2022-34172**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2781	A-JEN-JENK-060722/148
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	In Jenkins 2.340 through 2.355 (both inclusive) the tooltip of the build button in list views supports HTML without escaping the job display name, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission.	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2781	A-JEN-JENK-060722/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34173		
Observable Discrepancy	23-Jun-22	7.5	In Jenkins 2.355 and earlier, LTS 2.332.3 and earlier, an observable timing discrepancy on the login form allows distinguishing between login attempts with an invalid username, and login attempts with a valid username and wrong password, when using the Jenkins user database security realm. **CVE ID : CVE-2022-34174**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2566	A-JEN-JENK-060722/150
Incorrect Authorization	23-Jun-22	7.5	Jenkins 2.335 through 2.355 (both inclusive) allows attackers in some cases to bypass a protection mechanism, thereby directly accessing some view fragments containing sensitive information, bypassing any permission checks in the corresponding view. **CVE ID : CVE-2022-34175**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2777	A-JEN-JENK-060722/151
Product: jianliao_notification					
Cross-Site Request Forgery (CSRF)	23-Jun-22	6.5	A cross-site request forgery (CSRF) vulnerability in Jenkins Jianliao Notification Plugin	https://www.jenkins.io/security/advisory/2022-06-	A-JEN-JIAN-060722/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.1 and earlier allows attackers to send HTTP POST requests to an attacker-specified URL. **CVE ID : CVE-2022-34205**	22/#SECURITY-2240	
Missing Authorization	23-Jun-22	4.3	A missing permission check in Jenkins Jianliao Notification Plugin 1.1 and earlier allows attackers with Overall/Read permission to send HTTP POST requests to an attacker-specified URL. **CVE ID : CVE-2022-34206**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2240	A-JEN-JIAN-060722/153
Product: junit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	5.4	Jenkins JUnit Plugin 1119.va_a_5e9068da_d7 and earlier does not escape descriptions of test results, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Run/Update permission. **CVE ID : CVE-2022-34176**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2760	A-JEN-JUNI-060722/154
Product: maven_metadata					
Improper Neutralization of Input During	23-Jun-22	5.4	Jenkins Maven Metadata Plugin for Jenkins CI server Plugin 2.1 and earlier does not escape the	https://www.jenkins.io/security/advisory/2022-06-	A-JEN-MAVE-060722/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			name and description of List maven artifact versions parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. **CVE ID : CVE-2022-34190**	22/#SECURITY-2784	
Product: nested_view					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	Jenkins Nested View Plugin 1.20 through 1.25 (both inclusive) does not escape search parameters, resulting in a reflected cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2022-34182**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2768	A-JEN-NEST-060722/156
Product: ns-nd_integration_performance_publisher					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	5.4	Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.77 and earlier does not escape the name of NetStorm Test parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2784	A-JEN-NS-N-060722/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Item/Configure permission. **CVE ID : CVE-2022-34191**		
Product: ontrack					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	5.4	Jenkins ontrack Jenkins Plugin 4.0.0 and earlier does not escape the name of Ontrack: Multi Parameter choice, Ontrack: Parameter choice, and Ontrack: SingleParameter parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. **CVE ID : CVE-2022-34192**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2784	A-JEN-ONTR-060722/158
Product: package_version					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	5.4	Jenkins Package Version Plugin 1.0.1 and earlier does not escape the name of Package version parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2784	A-JEN-PACK-060722/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34193		
Product: pipeline					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jun-22	7.5	Jenkins Pipeline: Input Step Plugin 448.v37cea_9a_10a_70 and earlier archives files uploaded for `file` parameters for Pipeline `input` steps on the controller as part of build metadata, using the parameter name without sanitization as a relative path inside a build-related directory, allowing attackers able to configure Pipelines to create or replace arbitrary files on the Jenkins controller file system with attacker-specified content. **CVE ID : CVE-2022-34177**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2705	A-JEN-PIPE-060722/160
Product: readonly_parameter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	5.4	Jenkins Readonly Parameter Plugin 1.0.0 and earlier does not escape the name and description of Readonly String and Readonly Text parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2784	A-JEN-READ-060722/161

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers with Item/Configure permission. **CVE ID : CVE-2022-34194**		
Product: repository_connector					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	5.4	Jenkins Repository Connector Plugin 2.2.0 and earlier does not escape the name and description of Maven Repository Artifact parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. **CVE ID : CVE-2022-34195**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2784	A-JEN-REPO-060722/162
Product: rest_list_parameter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	5.4	Jenkins REST List Parameter Plugin 1.5.2 and earlier does not escape the name and description of REST list parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2784	A-JEN-REST-060722/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34196		
Product: sauce_ondemand					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	5.4	Jenkins Sauce OnDemand Plugin 1.204 and earlier does not escape the name and description of Sauce Labs Browsers parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. **CVE ID : CVE-2022-34197**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2784	A-JEN-SAUC-060722/164
Product: squash_tm_publisher					
Insufficiently Protected Credentials	23-Jun-22	6.5	Jenkins Squash TM Publisher (Squash4Jenkins) Plugin 1.0.0 and earlier stores passwords unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system. **CVE ID : CVE-2022-34213**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2089	A-JEN-SQUA-060722/165
Product: stash_branch_parameter					
Improper Neutralizat	23-Jun-22	5.4	Jenkins Stash Branch Parameter Plugin	https://www.jenkins.io/secu	A-JEN-STAS-060722/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			0.3.0 and earlier does not escape the name and description of Stash Branch parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. **CVE ID : CVE-2022-34198**	rity/advisory/2022-06-22/#SECURITY-2784	
Product: threadfix					
Cross-Site Request Forgery (CSRF)	23-Jun-22	6.5	A cross-site request forgery (CSRF) vulnerability in Jenkins ThreadFix Plugin 1.5.4 and earlier allows attackers to connect to an attacker-specified URL. **CVE ID : CVE-2022-34209**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2249	A-JEN-THRE-060722/167
Missing Authorization	23-Jun-22	6.5	A missing permission check in Jenkins ThreadFix Plugin 1.5.4 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL. **CVE ID : CVE-2022-34210**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2249	A-JEN-THRE-060722/168
Product: vrealize_orchestrator					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	23-Jun-22	6.5	A cross-site request forgery (CSRF) vulnerability in Jenkins vRealize Orchestrator Plugin 3.0 and earlier allows attackers to send an HTTP POST request to an attacker-specified URL. **CVE ID : CVE-2022-34211**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2279	A-JEN-VREA-060722/169
Missing Authorization	23-Jun-22	5.7	A missing permission check in Jenkins vRealize Orchestrator Plugin 3.0 and earlier allows attackers with Overall/Read permission to send an HTTP POST request to an attacker-specified URL. **CVE ID : CVE-2022-34212**	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2279	A-JEN-VREA-060722/170
Product: xunit					
Protection Mechanism Failure	23-Jun-22	9.1	Jenkins xUnit Plugin 3.0.8 and earlier implements an agent-to-controller message that creates a user-specified directory if it doesn't exist, and parsing files inside it as test results, allowing attackers able to control agent processes to create an arbitrary directory on the Jenkins controller or to obtain test results from existing	https://www.jenkins.io/security/advisory/2022-06-22/#SECURITY-2549	A-JEN-XUNI-060722/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files in an attacker-specified directory. **CVE ID : CVE-2022-34181**		
Vendor: jflyfox					
Product: jfinal_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	5.4	Jfinal CMS v5.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the keyword text field under the publish blog module. **CVE ID : CVE-2022-33113**	N/A	A-JFL-JFIN-060722/172
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jun-22	7.2	Jfinal CMS v5.1.0 was discovered to contain a SQL injection vulnerability via the attrVal parameter at /jfinal_cms/system/dict/list. **CVE ID : CVE-2022-33114**	N/A	A-JFL-JFIN-060722/173
Vendor: Jforum					
Product: jforum					
Cross-Site Request Forgery (CSRF)	16-Jun-22	8.8	JForum v2.8.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via http://target_host:port/jforum-2.8.0/jforum.page, which allows attackers to arbitrarily add admin accounts.	https://community.jforum.net/posts/list/248.page	A-JFO-JFOR-060722/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26173		
Vendor: kromit					
Product: titra					
Weak Password Requirements	16-Jun-22	9.8	Weak Password Requirements in GitHub repository kromitgmbh/titra prior to 0.78.1. **CVE ID : CVE-2022-2098**	https://github.com/kromitgmbh/titra/commit/7f09078a2ab88c35f2375c5f67bd0336c0e6c7a1, https://huntr.dev/bounties/a5d6c854-e158-49e9-bf40-bddc93dda7e6	A-KRO-TITR-060722/175
Vendor: libdwarf_project					
Product: libdwarf					
Out-of-bounds Read	23-Jun-22	8.1	There is a heap-based buffer over-read in libdwarf 0.4.0. This issue is related to dwarf_global_formref_b. **CVE ID : CVE-2022-34299**	https://github.com/davea42/libdwarf-code/commit/7ef09e1fc9ba07653dd078edb2408631c7969162	A-LIB-LIBD-060722/176
Vendor: libjxl_project					
Product: libjxl					
Reachable Assertion	19-Jun-22	6.5	libjxl 0.6.1 has an assertion failure in LowMemoryRenderPipeline::Init() in render_pipeline/low_memory_render_pipeline.cc. **CVE ID : CVE-2022-34000**	https://github.com/libjxl/libjxl/issues/1477	A-LIB-LIBJ-060722/177
Vendor: libpq_project					

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: libpq					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	17-Jun-22	7.5	All versions of package pg-native; all versions of package libpq are vulnerable to Denial of Service (DoS) when the addons attempt to cast the second argument to an array and fail. This happens for every non-array argument passed. **Note:** pg-native is a mere binding to npm's libpq library, which in turn has the addons and bindings to the actual C libpq library. This means that problems found in pg-native may transitively impact npm's libpq. **CVE ID : CVE-2022-25852**	https://snyk.io/vuln/SNYK-JS-LIBPQ-2392366, https://snyk.io/vuln/SNYK-JS-PGNATIVE-2392365	A-LIB-LIBP-060722/178
Vendor: maccms					
Product: maccms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	5.4	maccms8 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Server Group text field. **CVE ID : CVE-2022-31302**	N/A	A-MAC-MACC-060722/179
Improper Neutralization of Input During	21-Jun-22	5.4	maccms10 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the	N/A	A-MAC-MACC-060722/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Server Group text field. **CVE ID : CVE-2022-31303**		
Vendor: Mahara					
Product: mahara					
Incorrect Authorization	20-Jun-22	7.5	In Mahara 21.04 before 21.04.6, 21.10 before 21.10.4, and 22.04.2, files can sometimes be downloaded through thumb.php with no permission check. **CVE ID : CVE-2022-33913**	https://mahara.org/interaction/forum/topic.php?id=9138	A-MAH-MAHA-060722/181
Vendor: Mcafee					
Product: consumer_product_removal_tool					
Improper Privilege Management	20-Jun-22	7.8	Improper privilege management vulnerability in McAfee Consumer Product Removal Tool prior to version 10.4.128 could allow a local user to modify a configuration file and perform a LOLBin (Living off the land) attack. This could result in the user gaining elevated permissions and being able to execute arbitrary code, through not correctly checking the integrity of the configuration file. **CVE ID : CVE-2022-1823**	https://service.mcafee.com/?articleId=TS103318&page=shell&shell=article-view	A-MCA-CONS-060722/182

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Search Path Element	20-Jun-22	8.2	An uncontrolled search path vulnerability in McAfee Consumer Product Removal Tool prior to version 10.4.128 could allow a local attacker to perform a sideloading attack by using a specific file name. This could result in the user gaining elevated permissions and being able to execute arbitrary code as there were insufficient checks on the executable being signed by McAfee. **CVE ID : CVE-2022-1824**	https://service.mcafee.com/?articleId=TS103318&page=shell&shell=article-view	A-MCA-CONS-060722/183
Vendor: Microweber					
Product: microweber					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-22	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.2.17. **CVE ID : CVE-2022-2130**	https://github.com/microweber/microweber/commit/dbd37dda91911360db23269897c737e0abae2c24, https://huntr.dev/bounties/0142970a-5cb8-4dba-8bbc-4fa2f3bee65c	A-MIC-MICR-060722/184
Improper Neutralization of Input During	22-Jun-22	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.2.18.	https://huntr.dev/bounties/ac68e3fc-8cf1-4a62-90ee-95c4b2bad607	A-MIC-MICR-060722/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2022-2174**	, https://github.com/microweber/microweber/commit/c51285f791e48e536111cd57a9544ccbf7f33961	
Vendor: Mitel					
Product: mivoice_business					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jun-22	9.8	A vulnerability in the management interface of MiVoice Business through 9.3 PR1 and MiVoice Business Express through 8.0 SP3 PR3 could allow an unauthenticated attacker (that has network access to the management interface) to conduct a buffer overflow attack due to insufficient validation of URL parameters. A successful exploit could allow arbitrary code execution. **CVE ID : CVE-2022-31784**	https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-22-0005	A-MIT-MIVO-060722/186
Product: mivoice_business_express					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jun-22	9.8	A vulnerability in the management interface of MiVoice Business through 9.3 PR1 and MiVoice Business Express through 8.0 SP3 PR3 could allow an unauthenticated	https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-	A-MIT-MIVO-060722/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker (that has network access to the management interface) to conduct a buffer overflow attack due to insufficient validation of URL parameters. A successful exploit could allow arbitrary code execution. **CVE ID : CVE-2022-31784**	security-advisory-22-0005	
Vendor: moutjs					
Product: mout					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	17-Jun-22	7.5	This affects all versions of package mout. The deepFillIn function can be used to 'fill missing properties recursively', while the deepMixIn mixes objects into the target object, recursively mixing existing child objects as well. In both cases, the key used to access the target object recursively is not checked, leading to exploiting this vulnerability. **Note:** This vulnerability derives from an incomplete fix of [CVE-2020-7792](https://security.snyk.io/vuln/SNYK-JS-MOUT-1014544).	https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-2870622, https://snyk.io/vuln/SNYK-JS-MOUT-2342654, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-2870623, https://github.com/mout/mout/blob/master/src/object/deepMixIn.js	A-MOU-MOUT-060722/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21213		
Vendor: multi-page_toolkit_project					
Product: multi-page_toolkit					
Cross-Site Request Forgery (CSRF)	20-Jun-22	5.4	The Multi-page Toolkit WordPress plugin through 2.6 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack and lead to Stored Cross-Site Scripting due to the lack of sanitisation and escaping as well **CVE ID : CVE-2022-1818**	N/A	A-MUL-MULT-060722/189
Vendor: nic					
Product: knot_resolver					
Authentication Bypass by Spoofing	20-Jun-22	5.3	Knot Resolver through 5.5.1 may allow DNS cache poisoning when there is an attempt to limit forwarding actions by filters. **CVE ID : CVE-2022-32983**	https://knot-resolver.readthedocs.io/en/stable/modules-policy.html#forwarding, https://github.com/CZ-NIC/knot-resolver/commit/ccb9d9794db5eb757c33becf65cb1cf48ecfd968	A-NIC-KNOT-060722/190
Vendor: nukeviet					
Product: nukeviet					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	5.4	There is a Cross Site Scripting Stored (XSS) vulnerability in NukeViet CMS before 4.5.02. **CVE ID : CVE-2022-30874**	N/A	A-NUK-NUKE-060722/191
Vendor: online_discussion_forum_project					
Product: online_discussion_forum					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jun-22	9.8	Online Discussion Forum Site 1 was discovered to contain a blind SQL injection vulnerability via the component /odfs/posts/view_post.php. **CVE ID : CVE-2022-31296**	N/A	A-ONL-ONLI-060722/192
Vendor: online_discussion_forum_site_project					
Product: online_discussion_forum_site					
Cross-Site Request Forgery (CSRF)	16-Jun-22	6.5	An issue in the save_users() function of Online Discussion Forum Site 1 allows unauthenticated attackers to arbitrarily create or update user accounts. **CVE ID : CVE-2022-31294**	N/A	A-ONL-ONLI-060722/193
Authorization Bypass Through User-Controlled Key	16-Jun-22	7.5	An issue in the delete_post() function of Online Discussion Forum Site 1 allows unauthenticated attackers to arbitrarily delete posts.	N/A	A-ONL-ONLI-060722/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31295		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jun-22	7.2	Online Discussion Forum Site v1.0 is vulnerable to SQL Injection via /odfs/classes/Master.php?f=delete_team. **CVE ID : CVE-2022-31911**	N/A	A-ONL-ONLI-060722/195
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-22	4.8	Online Discussion Forum Site v1.0 is vulnerable to Cross Site Scripting (XSS) via /odfs/classes/Master.php?f=save_category, name. **CVE ID : CVE-2022-31913**	N/A	A-ONL-ONLI-060722/196
Vendor: online_fire_reporting_system_project					
Product: online_fire_reporting_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-22	4.8	Online Fire Reporting System v1.0 is vulnerable to Cross Site Scripting (XSS) via /ofrs/classes/Master.php. **CVE ID : CVE-2022-31906**	N/A	A-ONL-ONLI-060722/197
Vendor: online_ordering_system_project					
Product: online_ordering_system					
Improper Neutralization of Special Elements used in an	17-Jun-22	9.8	Online Ordering System v2.3.2 was discovered to contain a SQL injection vulnerability via	N/A	A-ONL-ONLI-060722/198

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			/ordering/index.php?q=category&search=. **CVE ID : CVE-2022-31355**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jun-22	9.8	Online Ordering System v2.3.2 was discovered to contain a SQL injection vulnerability via /ordering/admin/store/index.php?view=edit&id=. **CVE ID : CVE-2022-31356**	N/A	A-ONL-ONLI-060722/199
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jun-22	9.8	Online Ordering System v2.3.2 was discovered to contain a SQL injection vulnerability via /ordering/admin/inventory/index.php?view=edit&id=. **CVE ID : CVE-2022-31357**	N/A	A-ONL-ONLI-060722/200
Vendor: online_railway_reservation_system_project					
Product: online_railway_reservation_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jun-22	7.2	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /orrs/admin/reservations/view_details.php. **CVE ID : CVE-2022-33048**	N/A	A-ONL-ONLI-060722/201
Improper Neutralization of	21-Jun-22	7.2	Online Railway Reservation System v1.0 was discovered	N/A	A-ONL-ONLI-060722/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			to contain a SQL injection vulnerability via the id parameter at /orrs/admin/?page= user/manage_user. **CVE ID : CVE-2022-33049**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jun-22	7.2	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /orrs/admin/trains/ manage_train.php. **CVE ID : CVE-2022-33055**	N/A	A-ONL-ONLI-060722/203
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jun-22	7.2	Online Railway Reservation System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /orrs/admin/schedules/manage_schedule.php. **CVE ID : CVE-2022-33056**	N/A	A-ONL-ONLI-060722/204
Vendor: online_tutor_portal_site_project					
Product: online_tutor_portal_site					
Improper Neutralization of Input During Web Page Generation	16-Jun-22	4.8	Online Tutor Portal Site v1.0 is vulnerable to Cross Site Scripting (XSS). via /otps/classes/Master.php. **CVE ID : CVE-2022-31910**	N/A	A-ONL-ONLI-060722/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jun-22	7.2	Online Tutor Portal Site v1.0 is vulnerable to SQL Injection via /otps/classes/Master.php?f=delete_team. **CVE ID : CVE-2022-31912**	N/A	A-ONL-ONLI-060722/206
Vendor: opcfoundation					
Product: ua_.net_standard_stack					
Loop with Unreachable Exit Condition ('Infinite Loop')	16-Jun-22	7.5	An infinite loop in OPC UA .NET Standard Stack 1.04.368 allows a remote attackers to cause the application to hang via a crafted message. **CVE ID : CVE-2022-29862**	https://opcfoundation.org/security/, https://files.opcfoundation.org/SecurityBulletins/OPC%20Foundation%20Security%20Bulletin%20CVE-2022-29862.pdf	A-OPC-UA_.-060722/207
Allocation of Resources Without Limits or Throttling	16-Jun-22	7.5	OPC UA .NET Standard Stack 1.04.368 allows remote attacker to cause a crash via a crafted message that triggers excessive memory allocation. **CVE ID : CVE-2022-29863**	https://opcfoundation.org/security/, https://files.opcfoundation.org/SecurityBulletins/OPC%20Foundation%20Security%20Bulletin%20CVE-2022-29863.pdf	A-OPC-UA_.-060722/208
Uncontrolled Resource	16-Jun-22	7.5	OPC UA .NET Standard Stack 1.04.368 allows a remote attacker to	https://opcfoundation.org/security/, https://files.op	A-OPC-UA_.-060722/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			cause a server to crash via a large number of messages that trigger Uncontrolled Resource Consumption. **CVE ID : CVE-2022-29864**	cfoundation.org/SecurityBulletins/OPC%20Foundation%20Security%20Bulletin%20CVE-2022-29864.pdf	
Improper Authentication	16-Jun-22	7.5	OPC UA .NET Standard Stack allows a remote attacker to bypass the application authentication check via crafted fake credentials. **CVE ID : CVE-2022-29865**	https://opcfoundation.org/security/, https://files.opcfoundation.org/SecurityBulletins/OPC%20Foundation%20Security%20Bulletin%20CVE-2022-29865.pdf	A-OPC-UA_.-060722/210
Uncontrolled Resource Consumption	16-Jun-22	7.5	OPC UA .NET Standard Stack 1.04.368 allows a remote attacker to exhaust the memory resources of a server via a crafted request that triggers Uncontrolled Resource Consumption. **CVE ID : CVE-2022-29866**	https://opcfoundation.org/security/, https://files.opcfoundation.org/SecurityBulletins/OPC%20Foundation%20Security%20Bulletin%20CVE-2022-29866.pdf	A-OPC-UA_.-060722/211
Vendor: openlibrary					
Product: openlibrary					
Improper Neutralization of Input During Web Page	22-Jun-22	6.1	In openlibrary versions deploy-2016-07-0 through deploy-2021-12-22	https://github.com/internetarchive/openlibrary/pull/6597/commits/5460c8e8b517ef	A-OPE-OPEN-060722/212

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			are vulnerable to Reflected XSS. **CVE ID : CVE-2022-23081**	83c6a3b33654ba43ef0cbf051e	
Vendor: Openssl					
Product: openssl					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Jun-22	9.8	In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=9639817dac8bbbaa64d09efad7464ccc405527c7, https://www.openssl.org/news/secadv/20220621.txt, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=7a9c027159fe9e1bbc2cd38a8a2914bff0d5abd9	A-OPE-OPEN-060722/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze). **CVE ID : CVE-2022-2068**		
Vendor: Oracle					
Product: cloud_infrastructure					
N/A	17-Jun-22	4.9	Vulnerability in the Oracle Cloud Infrastructure product of Oracle Cloud Services. Easily exploitable vulnerability allows high privileged attacker with network access to compromise Oracle Cloud Infrastructure. Successful attacks of this vulnerability can result in unauthorized access to Oracle Cloud Infrastructure accessible data. All affected customers were notified of CVE-2022-21503 by Oracle. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS	N/A	A-ORA-CLOU-060722/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N) **CVE ID : CVE-2022-21503**		
Vendor: parseplatform					
Product: parse-server					
Improper Authentication	17-Jun-22	7.5	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 4.10.11 and 5.2.2, the certificate in the Parse Server Apple Game Center auth adapter not validated. As a result, authentication could potentially be bypassed by making a fake certificate accessible via certain Apple domains and providing the URL to that certificate in an authData object. Versions 4.0.11 and 5.2.2 prevent this by introducing a new \`rootCertificateUrl\` property to the Parse Server Apple Game Center auth adapter which takes the URL to the root certificate of Apple's Game Center authentication certificate. If no value is set, the \`rootCertificateUrl\`	https://github.com/parse-community/parse-server/security/advisories/GHSA-rh9j-f5f8-rvgc, https://github.com/parse-community/parse-server/pull/8054, https://github.com/parse-community/parse-server/commit/ba2b0a9cb9a568817a114b132a4c2e0911d76df1	A-PAR-PARS-060722/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			property defaults to the URL of the current root certificate as of May 27, 2022. Keep in mind that the root certificate can change at any time and that it is the developer's responsibility to keep the root certificate URL up-to-date when using the Parse Server Apple Game Center auth adapter. There are no known workarounds for this issue. **CVE ID : CVE-2022-31083**		
Vendor: pdf24_articles_to_pdf_project					
Product: pdf24_articles_to_pdf					
Cross-Site Request Forgery (CSRF)	20-Jun-22	6.5	The PDF24 Article To PDF WordPress plugin through 4.2.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID : CVE-2022-1827**	N/A	A-PDF-PDF2-060722/216
Cross-Site Request Forgery (CSRF)	20-Jun-22	6.5	The PDF24 Articles To PDF WordPress plugin through 4.2.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a	N/A	A-PDF-PDF2-060722/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logged in admin change them via a CSRF attack **CVE ID : CVE-2022-1828**		
Vendor: pg-native_project					
Product: pg-native					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	17-Jun-22	7.5	All versions of package pg-native; all versions of package libpq are vulnerable to Denial of Service (DoS) when the addons attempt to cast the second argument to an array and fail. This happens for every non-array argument passed. **Note:** pg-native is a mere binding to npm's libpq library, which in turn has the addons and bindings to the actual C libpq library. This means that problems found in pg-native may transitively impact npm's libpq. **CVE ID : CVE-2022-25852**	https://snyk.io/vuln/SNYK-JS-LIBPQ-2392366, https://snyk.io/vuln/SNYK-JS-PGNATIVE-2392365	A-PG--PG-N-060722/218
Vendor: Phoenixcontact					
Product: multiprog					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to the devices based on ProConOS/ProConOS eCLR in order to gain	https://cert.vde.com/en/advisories/VDE-2022-026/	A-PHO-MULT-060722/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			full control over the device. **CVE ID : CVE-2022-31801**		
Vendor: PHP					
Product: php					
Release of Invalid Pointer or Reference	16-Jun-22	9.8	In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when using Postgres database extension, supplying invalid parameters to the parametrized query may lead to PHP attempting to free memory using uninitialized data as pointers. This could lead to RCE vulnerability or denial of service. **CVE ID : CVE-2022-31625**	https://bugs.php.net/bug.php?id=81720	A-PHP-PHP-060722/220
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Jun-22	8.8	In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when pdo_mysql extension with mysqlnd driver, if the third party is allowed to supply host to connect to and the password for the connection, password of excessive length can trigger a buffer overflow in PHP, which can lead to a remote code	https://bugs.php.net/bug.php?id=81719	A-PHP-PHP-060722/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability. **CVE ID : CVE-2022-31626**		
Vendor: pmb_project					
Product: pmb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-22	6.1	PMB 7.3.10 allows reflected XSS via the id parameter in an lvl=author_see request to index.php. **CVE ID : CVE-2022-34328**	N/A	A-PMB-PMB-060722/222
Vendor: prison_management_system_project					
Product: prison_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/actions/view_action.php:4 **CVE ID : CVE-2022-32391**	N/A	A-PRI-PRIS-060722/223
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/actions/manage_action.php:4 **CVE ID : CVE-2022-32392**	N/A	A-PRI-PRIS-060722/224
Improper Neutralizat	24-Jun-22	8.8	Prison Management System v1.0 was	N/A	A-PRI-PRIS-060722/225

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/cells/view_cell.php:4 **CVE ID : CVE-2022-32393**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/inmates/view_inmate.php:3 **CVE ID : CVE-2022-32394**	N/A	A-PRI-PRIS-060722/226
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/crimes/manage_crime.php:4 **CVE ID : CVE-2022-32395**	N/A	A-PRI-PRIS-060722/227
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/visits/manage_visit.php:4 **CVE ID : CVE-2022-32396**	N/A	A-PRI-PRIS-060722/228
Improper Neutralization of	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain	N/A	A-PRI-PRIS-060722/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			a SQL injection vulnerability via the 'id' parameter at /pms/admin/visits/view_visit.php:4 **CVE ID : CVE-2022-32397**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/cells/manage_cell.php:4 **CVE ID : CVE-2022-32398**	N/A	A-PRI-PRIS-060722/230
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/crimes/view_crime.php:4 **CVE ID : CVE-2022-32399**	N/A	A-PRI-PRIS-060722/231
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	7.2	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/user/manage_user.php:4. **CVE ID : CVE-2022-32400**	N/A	A-PRI-PRIS-060722/232
Improper Neutralization of Special	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection	N/A	A-PRI-PRIS-060722/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			vulnerability via the 'id' parameter at /pms/admin/inmates/manage_privilege.php:4 **CVE ID : CVE-2022-32401**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/prisons/manage_prison.php:4 **CVE ID : CVE-2022-32402**	N/A	A-PRI-PRIS-060722/234
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/inmates/manage_record.php:4 **CVE ID : CVE-2022-32403**	N/A	A-PRI-PRIS-060722/235
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/inmates/manage_inmate.php:3 **CVE ID : CVE-2022-32404**	N/A	A-PRI-PRIS-060722/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jun-22	8.8	Prison Management System v1.0 was discovered to contain a SQL injection vulnerability via the 'id' parameter at /pms/admin/prisons /view_prison.php:4 **CVE ID : CVE-2022-32405**	N/A	A-PRI-PRIS-060722/237
Vendor: proietti					
Product: planet_time_enterprise					
Use of Hard-coded Credentials	17-Jun-22	9.8	Proietti Tech srl Planet Time Enterprise 4.2.0.1,4.2.0.0,4.1.0.0, 4.0.0.0,3.3.1.0,3.3.0.0 is vulnerable to Remote code execution via the Viewstate parameter. **CVE ID : CVE-2022-30422**	N/A	A-PRO-PLAN-060722/238
Vendor: querymen_project					
Product: querymen					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	17-Jun-22	7.5	All versions of package querymen are vulnerable to Prototype Pollution if the parameters of exported function handler(type, name, fn) can be controlled by users without any sanitization. Note: This vulnerability derives from an incomplete fix of [CVE-2020-7600](https://security.snyk.io/vuln/SNYK-	https://snyk.io /vuln/SNYK-JS-QUERYMEN-2391488	A-QUE-QUER-060722/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JS-QUERYMEN-559867). **CVE ID : CVE-2022-25871**		
Vendor: rangerstudio					
Product: directus					
Server-Side Request Forgery (SSRF)	22-Jun-22	4.3	In directus versions v9.0.0-beta.2 through 9.6.0 are vulnerable to server-side request forgery (SSRF) in the media upload functionality which allows a low privileged user to perform internal network port scans. **CVE ID : CVE-2022-23080**	https://github.com/directus/directus/commit/6da3f1ed5034115b1da00440008351bf0d808d83	A-RAN-DIRE-060722/240
Vendor: Redhat					
Product: amq_broker					
Incorrect Default Permissions	21-Jun-22	8.8	A flaw was found in AMQ Broker Operator 7.9.4 installed via UI using OperatorHub where a low-privilege user that has access to the namespace where the AMQ Operator is deployed has access to clusterwide edit rights by checking the secrets. The service account used for building the Operator gives more permission than expected and an attacker could benefit from it. This requires	https://bugzilla.redhat.com/show_bug.cgi?id=2089406#c4	A-RED-AMQ_-060722/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			at least an already compromised low-privilege account or insider attack. **CVE ID : CVE-2022-1833**		
Vendor: redis					
Product: redis					
Missing Release of Memory after Effective Lifetime	23-Jun-22	7.5	Redis v7.0 was discovered to contain a memory leak via the component streamGetEdgeID. **CVE ID : CVE-2022-33105**	https://github.com/redis/redis/commit/4a7a4e42db8ff757cdf3f4a824f66426036034ef, https://github.com/redis/redis/pull/10753	A-RED-REDI-060722/242
Vendor: rescue_dispatch_management_system_project					
Product: rescue_dispatch_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jun-22	9.8	Rescue Dispatch Management System v1.0 is vulnerable to SQL Injection via \rdms\admin?page=user\manage_user&id=. **CVE ID : CVE-2022-31941**	N/A	A-RES-RESC-060722/243
Vendor: seamless_donations_project					
Product: seamless_donations					
Cross-Site Request Forgery (CSRF)	20-Jun-22	6.5	The Seamless Donations WordPress plugin before 5.1.9 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin	N/A	A-SEA-SEAM-060722/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			change them via a CSRF attack **CVE ID : CVE-2022-1610**		
Vendor: Siemens					
Product: wincc_open_architecture					
Improper Authentication	21-Jun-22	9.8	A vulnerability has been identified in SIMATIC WinCC OA V3.16 (All versions in default configuration), SIMATIC WinCC OA V3.17 (All versions in non-default configuration), SIMATIC WinCC OA V3.18 (All versions in non-default configuration). Affected applications use client-side only authentication, when neither server-side authentication (SSA) nor Kerberos authentication is enabled. In this configuration, attackers could impersonate other users or exploit the client-server protocol without being authenticated. **CVE ID : CVE-2022-33139**	https://cert-portal.siemens.com/productcert/pdf/ssa-111512.pdf	A-SIE-WINC-060722/245
Vendor: simple_bakery_shop_management_system_project					
Product: simple_bakery_shop_management_system					
Improper Neutralizat	23-Jun-22	4.8	Multiple cross-site scripting (XSS)	N/A	A-SIM-SIMP-060722/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			vulnerabilities in /bsms/?page=manage_account of Simple Bakery Shop Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Username or Full Name fields. **CVE ID : CVE-2022-32987**		
Vendor: Southrivertech					
Product: titan_ftp_server_nextgen					
Use of Hard-coded Credentials	19-Jun-22	9.8	An issue was discovered in TitanFTP (aka Titan FTP) NextGen before 1.2.1050. There is Remote Code Execution due to a hardcoded password for the sa account on the Microsoft SQL Express 2019 instance installed by default during TitanFTP NextGen installation, aka NX-I674 (sub-issue 1). NOTE: as of 2022-06-21, the 1.2.1050 release corrects this vulnerability in a new installation, but not in an upgrade installation. **CVE ID : CVE-2022-34005**	https://www.southrivertech.com/software/nextgen/titanftp/en/relnotes.pdf	A-SOU-TITA-060722/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	19-Jun-22	7.8	An issue was discovered in TitanFTP (aka Titan FTP) NextGen before 1.2.1050. When installing, Microsoft SQL Express 2019 installs by default with an SQL instance running as SYSTEM with BUILTIN\Users as sysadmin, thus enabling unprivileged Windows users to execute commands locally as NT AUTHORITY\SYSTEM , aka NX-I674 (sub-issue 2). NOTE: as of 2022-06-21, the 1.2.1050 release corrects this vulnerability in a new installation, but not in an upgrade installation. **CVE ID : CVE-2022-34006**	https://www.southrivertech.com/software/nextgen/titanftp/en/relnotes.pdf	A-SOU-TITA-060722/248
Vendor: sr.solutions					
Product: usertakeover					
N/A	21-Jun-22	4.3	The UserTakeOver plugin before 4.0.1 for ILIAS allows an attacker to list all users via the search function. **CVE ID : CVE-2022-31478**	N/A	A-SR.-USER-060722/249
Vendor: student_registration_and_fee_payment_system_project					
Product: student_registration_and_fee_payment_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jun-22	7.2	Student Registration and Fee Payment System v1.0 is vulnerable to SQL Injection via /scms/student.php. **CVE ID : CVE-2022-31908**	N/A	A-STU-STUD-060722/250
Vendor: Suse					
Product: manager_server					
Observable Response Discrepancy	22-Jun-22	5.3	A Observable Response Discrepancy vulnerability in spacewalk-java of SUSE Manager Server 4.1, SUSE Manager Server 4.2 allows remote attackers to discover valid usernames. This issue affects: SUSE Manager Server 4.1 spacewalk-java versions prior to 4.1.46-1. SUSE Manager Server 4.2 spacewalk-java versions prior to 4.2.37-1. **CVE ID : CVE-2022-31248**	https://bugzilla.suse.com/show_bug.cgi?id=1199629	A-SUS-MANA-060722/251
Vendor: tandoor					
Product: recipes					
Server-Side Request Forgery (SSRF)	19-Jun-22	6.5	In Recipes, versions 0.9.1 through 1.2.5 are vulnerable to Server Side Request Forgery (SSRF), in the “Import Recipe” functionality. When	https://www.mend.io/vulnerability-database/CVE-2022-23071, https://github.com/TandoorR	A-TAN-RECI-060722/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker enters the localhost URL, a low privileged attacker can access/read the internal file system to access sensitive information. **CVE ID : CVE-2022-23071**	ecipes/recipes/commit/d48fe26a3529cc1ee903ffb2758dfd8f7efaba8c	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	5.4	In Recipes, versions 1.0.5 through 1.2.5 are vulnerable to Stored Cross-Site Scripting (XSS), in “Add to Cart” functionality. When a victim accesses the food list page, then adds a new Food with a malicious javascript payload in the ‘Name’ parameter and clicks on the Add to Shopping Cart icon, an XSS payload will trigger. A low privileged attacker will have the victim's API key and can lead to admin's account takeover. **CVE ID : CVE-2022-23072**	https://www.mend.io/vulnerability-database/CVE-2022-23072, https://github.com/TandoorRecipes/recipes/commit/7b2117c0190d4f541ba4cc7ee4122f04738c4ac6	A-TAN-RECI-060722/253
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	5.4	In Recipes, versions 1.0.5 through 1.2.5 are vulnerable to Stored Cross-Site Scripting (XSS), in copy to clipboard functionality. When a victim accesses the food list page, then adds a new Food with	https://github.com/TandoorRecipes/recipes/commit/7b2117c0190d4f541ba4cc7ee4122f04738c4ac6	A-TAN-RECI-060722/254

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a malicious javascript payload in the ‘Name’ parameter and clicks on the clipboard icon, an XSS payload will trigger. A low privileged attacker will have the victim's API key and can lead to admin's account takeover. **CVE ID : CVE-2022-23073**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	5.4	In Recipes, versions 0.17.0 through 1.2.5 are vulnerable to Stored Cross-Site Scripting (XSS), in the ‘Name’ field of Keyword, Food and Unit components. When a victim accesses the Keyword/Food/Unit endpoints, the XSS payload will trigger. A low privileged attacker will have the victim's API key and can lead to admin's account takeover. **CVE ID : CVE-2022-23074**	https://github.com/TandoorRecipes/recipes/commit/7b2117c0190d4f541ba4cc7ee4122f04738c4ac6	A-TAN-RECI-060722/255
Vendor: Tenable					
Product: nessus					
N/A	21-Jun-22	8.8	An authenticated attacker could create an audit file that bypasses PowerShell cmdlet checks and executes commands	https://www.tenable.com/security/tns-2022-11	A-TEN-NESS-060722/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with administrator privileges. **CVE ID : CVE-2022-32973**		
N/A	21-Jun-22	6.5	An authenticated attacker could read arbitrary files from the underlying operating system of the scanner using a custom crafted compliance audit file without providing any valid SSH credentials. **CVE ID : CVE-2022-32974**	https://www.tenable.com/security/tns-2022-11	A-TEN-NESS-060722/257
Vendor: thenewsletterplugin					
Product: newsletter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-22	4.8	The Newsletter WordPress plugin before 7.4.6 does not escape and sanitise the preheader_text setting, which could allow high privilege users to perform Stored Cross-Site Scripting attacks when the unfilteredhtml is disallowed **CVE ID : CVE-2022-1889**	N/A	A-THE-NEWS-060722/258
Vendor: tinyexr_project					
Product: tinyexr					
Out-of-bounds Read	23-Jun-22	8.8	In tinyexr 1.0.1, there is a heap-based buffer over-read in	N/A	A-TIN-TINY-060722/259

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tinyexr::DecodePixel Data. **CVE ID : CVE-2022-34300**		
Vendor: tribe29					
Product: checkmk					
Incorrect Default Permissions	17-Jun-22	7.8	A permission issue affects users that deployed the shipped version of the Checkmk Debian package. Packages created by the agent bakery (enterprise editions only) were not affected. Using the shipped version of the agents, the maintainer scripts located at /var/lib/dpkg/info/ will be owned by the user and the group with ID 1001. If such a user exists on the system, they can change the content of these files (which are then executed by root). This leads to a local privilege escalation on the monitored host. Version 1.6 through 1.6.9p29, version 2.0 through 2.0.0p26, version 2.1 through 2.1.0p3, and version 2.2.0i1 are affected. **CVE ID : CVE-2022-33912**	https://checkmk.com/werk/14098	A-TRI-CHEC-060722/260
Vendor: trudesk_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: trudesk					
Improper Privilege Management	20-Jun-22	9.8	Incorrect Use of Privileged APIs in GitHub repository polonel/trudesk prior to 1.2.4. **CVE ID : CVE-2022-2023**	https://huntr.dev/bounties/0f35b1d3-56e6-49e4-bc5a-830f52e094b3, https://github.com/polonel/trudesk/commit/83fd5a89319ba2c2f5934722e39b08aba9b3a4ac	A-TRU-TRUD-060722/261
Unrestricted Upload of File with Dangerous Type	20-Jun-22	9.8	Unrestricted Upload of File with Dangerous Type in GitHub repository polonel/trudesk prior to 1.2.4. **CVE ID : CVE-2022-2128**	https://github.com/polonel/trudesk/commit/fb2ef82b0a39d0a560a261e07c3c73ba25332ecb, https://huntr.dev/bounties/ec40ec76-c7db-4384-a33b-024f3dd21d75	A-TRU-TRUD-060722/262
Vendor: underconstruction_project					
Product: underconstruction					
Cross-Site Request Forgery (CSRF)	20-Jun-22	4.3	The underConstruction WordPress plugin before 1.20 does not have CSRF check in place when deactivating the construction mode, which could allow attackers to make a logged in admin perform such action via a CSRF attack	N/A	A-UND-UNDE-060722/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1895		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-22	4.8	The underConstruction WordPress plugin before 1.21 does not sanitise or escape the "Display a custom page using your own HTML" setting before outputting it, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiletred_html capability is disallowed. **CVE ID : CVE-2022-1896**	N/A	A-UND-UNDE-060722/264
Vendor: unioncms_project					
Product: unioncms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	5.4	Unioncms v1.0.13 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Default settings. **CVE ID : CVE-2022-25585**	N/A	A-UNI-UNIO-060722/265
Vendor: very_simple_contact_form_project					
Product: very_simple_contact_form					
Incorrect Authorization	20-Jun-22	7.5	The Very Simple Contact Form WordPress plugin before 11.6 exposes the solution to the captcha in the rendered contact form, both as hidden	N/A	A-VER-VERY-060722/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input fields and as plain text in the page, making it very easy for bots to bypass the captcha check, rendering the page a likely target for spam bots. **CVE ID : CVE-2022-1801**		
Vendor: VIM					
Product: vim					
Buffer Over-read	20-Jun-22	7.8	Buffer Over-read in function grab_file_name in GitHub repository vim/vim prior to 8.2.4956. This vulnerability is capable of crashing the software, memory modification, and possible remote execution. **CVE ID : CVE-2022-1720**	https://github.com/vim/vim/commit/395bd1f6d3edc9f7edb5d1f2d7deaf5a9e3ab93c, https://huntr.dev/bounties/5ccfb386-7eb9-46e5-98e5-243ea4b358a8	A-VIM-VIM-060722/267
Buffer Over-read	19-Jun-22	7.8	Buffer Over-read in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-2124**	https://github.com/vim/vim/commit/2f074f4685897ab7212e25931eeeb0212292829f, https://huntr.dev/bounties/8e9e056d-f733-4540-98b6-414bf36e0b42	A-VIM-VIM-060722/268
Heap-based	19-Jun-22	7.8	Heap-based Buffer Overflow in GitHub	https://huntr.dev/bounties/17dab24d-beec-464d-	A-VIM-VIM-060722/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			repository vim/vim prior to 8.2. **CVE ID : CVE-2022-2125**	9a72-5b6b11283705, https://github.com/vim/vim/commit/0e8e938d497260dd57be67b4966cb27a5f72376f	
Out-of-bounds Read	19-Jun-22	7.8	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-2126**	https://github.com/vim/vim/commit/156d3911952d73b03d7420dc3540215247db0fe8, https://huntr.dev/bounties/8d196d9b-3d10-41d2-9f70-8ef0d08c946e	A-VIM-VIM-060722/270
Out-of-bounds Write	19-Jun-22	7.8	Out-of-bounds Write in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-2129**	https://huntr.dev/bounties/3aaf06e7-9ae1-454d-b8ca-8709c98e5352 , https://github.com/vim/vim/commit/d6211a52ab9f53b82f884561ed43d2fe4d24ff7d	A-VIM-VIM-060722/271
Buffer Over-read	23-Jun-22	8.8	Buffer Over-read in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-2175**	https://github.com/vim/vim/commit/6046aded8da002b08d380db29de2ba0268b6616e, https://huntr.dev/bounties/7f0481c2-	A-VIM-VIM-060722/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				8b57-4324-b47c-795d1ea67e55	
Heap-based Buffer Overflow	23-Jun-22	7.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-2182**	https://github.com/vim/vim/commit/f7c7c3fad6d2135d558f3b36d0d1a943118aeb5e, https://huntr.dev/bounties/238d8650-3beb-4831-a8f7-6f0b597a6fb8	A-VIM-VIM-060722/273
Out-of-bounds Read	23-Jun-22	7.8	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-2183**	https://github.com/vim/vim/commit/8eba2bd291b347e3008aa9e565652d51ad638cfa, https://huntr.dev/bounties/d74ca3f9-380d-4c0a-b61c-11113cc98975	A-VIM-VIM-060722/274
Vendor: Vmware					
Product: spring_cloud_function					
Allocation of Resources Without Limits or Throttling	21-Jun-22	7.5	In Spring Cloud Function versions prior to 3.2.6, it is possible for a user who directly interacts with framework provided lookup functionality to cause a denial-of-service condition due to the caching issue in the Function Catalog	https://tanzu.vmware.com/security/cve-2022-22979	A-VMW-SPRI-060722/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component of the framework. **CVE ID : CVE-2022-22979**		
Product: vmware_hcx					
Exposure of Sensitive Information to an Unauthorized Actor	16-Jun-22	6.5	VMware HCX update addresses an information disclosure vulnerability. A malicious actor with network user access to the VMware HCX appliance may be able to gain access to sensitive information. **CVE ID : CVE-2022-22953**	https://www.vmware.com/security/advisories/VMSA-2022-0017.html	A-VMW-VMWA-060722/276
Vendor: webnus					
Product: modern_events_calendar_lite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-22	5.4	Cross-site scripting vulnerability in Modern Events Calendar Lite versions prior to 6.3.0 allows remote an authenticated attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2022-30533**	N/A	A-WEB-MODE-060722/277
Vendor: wire					
Product: wire					
Reachable Assertion	23-Jun-22	6.5	wire-ios is an iOS client for the Wire secure messaging application. Invalid accent colors of Wire communication	https://github.com/wireapp/wire-ios/commit/caa0e27dbe51f9edfda8c7a9f01	A-WIR-WIRE-060722/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			partners may render the iOS Wire Client partially unusable by causing it to crash multiple times on launch. These invalid accent colors can be used by and sent between Wire users. The root cause was an unnecessary assert statement when converting an integer value into the corresponding enum value, causing an exception instead of a fallback to a default value. This issue is fixed in [wire-ios](https://github.com/wireapp/wire-ios/commit/caa0e27dbe51f9edfda8c7a9f017d93b8cfddefb) and in Wire for iOS 3.100. There is no workaround available, but users may use other Wire clients (such as the [web app](https://app.wire.com)) to continue using Wire, or upgrade their client. **CVE ID : CVE-2022-31009**	7d93b8cfddefb , https://github.com/wireapp/wire-ios/security/advisories/GHSA-83m6-p7x5-925j	
Vendor: wiris					
Product: mathtype					
Improper Limitation of a	16-Jun-22	7.5	Wiris Mathtype v7.28.0 was discovered to contain	https://github.com/wiris/moodle-	A-WIR-MATH-060722/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			a path traversal vulnerability in the resourceFile parameter. This vulnerability is exploited via a crafted request to the resource handler. **CVE ID : CVE-2022-31372**	filter_wiris/commit/037ce9c1d9b9642689a332b6ebee8eaf0a737576	
Vendor: wp-email_project					
Product: wp-email					
Authorization Bypass Through User-Controlled Key	20-Jun-22	7.5	The WP-EMail WordPress plugin before 2.69.0 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based anti-spamming restrictions. **CVE ID : CVE-2022-1614**	N/A	A-WP--WP-E-060722/280
Cross-Site Request Forgery (CSRF)	20-Jun-22	6.5	The WP-EMail WordPress plugin before 2.69.0 does not protect its log deletion functionality with nonce checks, allowing attacker to make a logged in admin delete logs via a CSRF attack **CVE ID : CVE-2022-1630**	N/A	A-WP--WP-E-060722/281
Vendor: wp-experts					
Product: custom_share_buttons_with_floating_sidebar					

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-22	4.8	The Custom Share Buttons with Floating Sidebar WordPress plugin before 4.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-1717**	N/A	A-WP--CUST-060722/282
Vendor: wplite_project					
Product: wplite					
Cross-Site Request Forgery (CSRF)	20-Jun-22	6.5	The WPlite WordPress plugin through 1.3.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID : CVE-2022-1831**	N/A	A-WPL-WPLI-060722/283
Vendor: wpreviewslider					
Product: wp_zillow_review_slider					
Improper Neutralization of Input During Web Page Generation	20-Jun-22	4.8	The WP Zillow Review Slider WordPress plugin before 2.4 does not escape a settings, which could allow high privilege users to	N/A	A-WPR-WP_Z-060722/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite) **CVE ID : CVE-2022-1915**		
Vendor: Yuba					
Product: U5cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jun-22	6.1	u5cms version 8.3.5 is vulnerable to Cross Site Scripting (XSS). When a user accesses the default home page if the parameter passed in is http://127.0.0.1/?"Onmouseover=%27tzgl (96502)%27bad=", it can cause html injection. **CVE ID : CVE-2022-32442**	N/A	A-YUB-U5CM-060722/285
URL Redirection to Untrusted Site ('Open Redirect')	17-Jun-22	6.1	An issue was discovered in u5cms verion 8.3.5 There is a URL redirection vulnerability that can cause a user's browser to be redirected to another site via /loginsave.php. **CVE ID : CVE-2022-32444**	N/A	A-YUB-U5CM-060722/286
Vendor: zhyd					
Product: oneblog					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	23-Jun-22	4.3	OneBlog v2.3.4 was discovered to contain a Server-Side Request Forgery (SSRF) vulnerability via the parameter entryUrls. **CVE ID : CVE-2022-34011**	N/A	A-ZHY-ONEB-060722/287
Incorrect Permission Assignment for Critical Resource	23-Jun-22	6.5	Insecure permissions in OneBlog v2.3.4 allows low-level administrators to reset the passwords of high-level administrators who hold greater privileges. **CVE ID : CVE-2022-34012**	N/A	A-ZHY-ONEB-060722/288
Server-Side Request Forgery (SSRF)	23-Jun-22	4.3	OneBlog v2.3.4 was discovered to contain a Server-Side Request Forgery (SSRF) vulnerability via the Logo parameter under the Link module. **CVE ID : CVE-2022-34013**	N/A	A-ZHY-ONEB-060722/289
Vendor: zoo_management_system_project					
Product: zoo_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-22	5.4	Zoo Management System v1.0 is vulnerable to Cross Site Scripting (XSS) via zms/admin/public_html/save_animal?an_id=24. **CVE ID : CVE-2022-31914**	N/A	A-ZOO-ZOO_-060722/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Hardware					
Vendor: ABB					
Product: rex640_pcl1					
Incorrect Permission Assignment for Critical Resource	21-Jun-22	6.5	Incorrect Permission Assignment for Critical Resource vulnerability in ABB REX640 PCL1, REX640 PCL2, REX640 PCL3 allows an authenticated attacker to launch an attack against the user database file and try to take control of an affected system node. **CVE ID : CVE-2022-1596**	https://search.abb.com/library/Download.aspx?DocumentID=2NGA001421	H-ABB-REX6-060722/291
Product: rex640_pcl2					
Incorrect Permission Assignment for Critical Resource	21-Jun-22	6.5	Incorrect Permission Assignment for Critical Resource vulnerability in ABB REX640 PCL1, REX640 PCL2, REX640 PCL3 allows an authenticated attacker to launch an attack against the user database file and try to take control of an affected system node. **CVE ID : CVE-2022-1596**	https://search.abb.com/library/Download.aspx?DocumentID=2NGA001421	H-ABB-REX6-060722/292
Product: rex640_pcl3					
Incorrect Permission Assignment for	21-Jun-22	6.5	Incorrect Permission Assignment for Critical Resource vulnerability in ABB	https://search.abb.com/library/Download.aspx?DocumentI	H-ABB-REX6-060722/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			REX640 PCL1, REX640 PCL2, REX640 PCL3 allows an authenticated attacker to launch an attack against the user database file and try to take control of an affected system node. **CVE ID : CVE-2022-1596**	D=2NGA001421	
Vendor: anker					
Product: eufy_homebase_2					
Use After Free	17-Jun-22	9.8	A use-after-free vulnerability exists in the mips_collector appsrv_server functionality of Anker Eufy Homebase 2 2.1.8.5h. A specially-crafted set of network packets can lead to remote code execution. The device is exposed to attacks from the network. **CVE ID : CVE-2022-21806**	N/A	H-ANK-EUFY-060722/294
Vendor: Asus					
Product: rt-n53					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Jun-22	9.8	ASUS RT-N53 3.0.0.4.376.3754 has a command injection vulnerability in the SystemCmd parameter of the apply.cgi interface. **CVE ID : CVE-2022-31874**	N/A	H-ASU-RT-N-060722/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Cisco					
Product: ws-c2940-8tf-s					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-22	6.1	** Unsupported When Assigned ** Cisco Catalyst 2940 Series Switches provided by Cisco Systems, Inc. contain a reflected cross-site scripting vulnerability regarding error page generation. An arbitrary script may be executed on the web browser of the user who is using the product. The affected firmware is prior to 12.2(50)SY released in 2011, and Cisco Catalyst 2940 Series Switches have been retired since January 2015. **CVE ID : CVE-2022-31734**	https://www.cisco.com/c/en/us/obsolete/switches/cisco-catalyst-2940-series-switches.html	H-CIS-WS-C-060722/296
Product: ws-c2940-8tt-s					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-22	6.1	** Unsupported When Assigned ** Cisco Catalyst 2940 Series Switches provided by Cisco Systems, Inc. contain a reflected cross-site scripting vulnerability regarding error page generation. An arbitrary script may be executed on the web browser of the user who is using the product. The affected	https://www.cisco.com/c/en/us/obsolete/switches/cisco-catalyst-2940-series-switches.html	H-CIS-WS-C-060722/297

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware is prior to 12.2(50)SY released in 2011, and Cisco Catalyst 2940 Series Switches have been retired since January 2015. **CVE ID : CVE-2022-31734**		
Vendor: contec					
Product: sv-cpt-mc310					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	6.1	SolarView Compact v6.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component Solar_AiConf.php. **CVE ID : CVE-2022-31373**	N/A	H-CON-SV-C-060722/298
Unrestricted Upload of File with Dangerous Type	21-Jun-22	9.8	An arbitrary file upload vulnerability /images/background/1.php in of SolarView Compact 6.0 allows attackers to execute arbitrary code via a crafted php file. **CVE ID : CVE-2022-31374**	N/A	H-CON-SV-C-060722/299
Vendor: Fujitsu					
Product: eternus_cs8000					
Improper Neutralization of Special Elements used in an OS Command	20-Jun-22	9.8	An issue was discovered on Fujitsu ETERNUS CentricStor CS8000 (Control Center) devices before 8.1A SP02 P04. The vulnerability resides in the	https://support.ts.fujitsu.com/ProductSecurity/content/Fujitsu-PSIRT-PSS-IS-2022-050316-	H-FUJ-ETER-060722/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			requestTempFile function in hw_view.php. An attacker is able to influence the unitName POST parameter and inject special characters such as semicolons, backticks, or command-substitution sequences in order to force the application to execute arbitrary commands. **CVE ID : CVE-2022-31794**	Security-Notice-SF.pdf	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jun-22	9.8	An issue was discovered on Fujitsu ETERNUS CentricStor CS8000 (Control Center) devices before 8.1A SP02 P04. The vulnerability resides in the grel_finfo function in grel.php. An attacker is able to influence the username (user), password (pw), and file-name (file) parameters and inject special characters such as semicolons, backticks, or command-substitution sequences in order to force the application to execute arbitrary commands.	https://support.ts.fujitsu.com/ProductSecurity/content/Fujitsu-PSIRT-PSS-IS-2022-050316-Security-Notice-SF.pdf	H-FUJ-ETER-060722/301

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31795		
Vendor: Mercurycom					
Product: mipc451-4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jun-22	8.8	MERCURY MIPC451-4 1.0.22 Build 220105 Rel.55642n was discovered to contain a remote code execution (RCE) vulnerability which is exploitable via a crafted POST request. **CVE ID : CVE-2022-31849**	N/A	H-MER-MIPC-060722/302
Vendor: mi					
Product: xiaomi_lamp_1					
Authentication Bypass by Capture-replay	16-Jun-22	8.8	Xiaomi Lamp 1 v2.0.4_0066 was discovered to be vulnerable to replay attacks. This allows attackers to to bypass the expected access restrictions and gain control of the switch and other functions via a crafted POST request. **CVE ID : CVE-2022-31277**	N/A	H-MI-XIAO-060722/303
Vendor: Netgear					
Product: wnap320					
Incorrect Authorization	17-Jun-22	5.3	netgear wnap320 router WNAP320_V2.0.3_firmware is vulnerable to Incorrect Access Control via /recreate.php, which	https://www.netgear.com/about/security/	H-NET-WNAP-060722/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can leak all users cookies. **CVE ID : CVE-2022-31876**		
Vendor: Nuuo					
Product: nvrsolo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	6.1	NUUO Network Video Recorder NVRsolo v03.06.02 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via login.php. **CVE ID : CVE-2022-33119**	N/A	H-NUU-NVRS-060722/305
Vendor: Phoenixcontact					
Product: axc_1050					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-AXC_-060722/306
Product: axc_1050_xc					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device.	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-AXC_-060722/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31800		
Product: axc_3050					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-AXC_-060722/308
Product: fc_350_pci_eth					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-FC_3-060722/309
Product: ilc1x0					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-ILC1-060722/310
Product: ilc1x1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-ILC1-060722/311
Product: ilc_1x1_gsm\/gprs					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-ILC_-060722/312
Product: ilc_3xx					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-ILC_-060722/313
Product: pc_worx_rt_basic					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-PC_W-060722/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**		
Product: pc_worx_srt					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-PC_W-060722/315
Product: rfc_430_eth-ib					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-RFC_-060722/316
Product: rfc_450_eth-ib					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device.	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-RFC_-060722/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31800		
Product: rfc_460r_pn_3tx					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-RFC_-060722/318
Product: rfc_460r_pn_3tx-s					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-RFC_-060722/319
Product: rfc_470s_pn_3tx					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-RFC_-060722/320
Product: rfc_470_pn_3tx					

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-RFC_-060722/321
Product: rfc_480s_pn_4tx					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	H-PHO-RFC_-060722/322
Vendor: quectel					
Product: rg502q-ea					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Jun-22	9.8	The Quectel RG502Q-EA modem before 2022-02-23 allow OS Command Injection. **CVE ID : CVE-2022-26147**	N/A	H-QUE-RG50-060722/323
Vendor: Tenda					
Product: hg9					
Improper Neutralization of	16-Jun-22	8.8	Tenda ONT GPON AC1200 Dual band WiFi HG9 v1.0.1 is	N/A	H-TEN-HG9-060722/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection via the Ping function. **CVE ID : CVE-2022-30023**		
Vendor: Trendnet					
Product: tew-831dr					
Weak Password Requirements	16-Jun-22	8.8	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The default pre-shared key for the Wi-Fi networks is the same for every router except for the last four digits. The device default pre-shared key for both 2.4 GHz and 5 GHz networks can be guessed or brute-forced by an attacker within range of the Wi-Fi network. **CVE ID : CVE-2022-30325**	N/A	H-TRE-TEW--060722/325
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-22	5.4	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The network pre-shared key field on the web interface is vulnerable to XSS. An attacker can use a simple XSS payload to crash the basic.config page of the web interface.	N/A	H-TRE-TEW--060722/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30326		
Cross-Site Request Forgery (CSRF)	16-Jun-22	6.5	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The web interface is vulnerable to CSRF. An attacker can change the pre-shared key of the Wi-Fi router if the interface's IP address is known. **CVE ID : CVE-2022-30327**	N/A	H-TRE-TEW--060722/327
Cross-Site Request Forgery (CSRF)	16-Jun-22	6.5	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The username and password setup for the web interface does not require entering the existing password. A malicious user can change the username and password of the interface. **CVE ID : CVE-2022-30328**	N/A	H-TRE-TEW--060722/328
Improper Neutralization of Special Elements used in an OS Command	16-Jun-22	9.8	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. An OS injection vulnerability exists within the web interface, allowing an	N/A	H-TRE-TEW--060722/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			attacker with valid credentials to execute arbitrary shell commands. **CVE ID : CVE-2022-30329**		
Product: tv-ip110wn					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jun-22	6.1	Trendnet IP-110wn camera fw_tv-ip110wn_v2(1.2.2.68) has an XSS vulnerability via the prefix parameter in /admin/general.cgi. **CVE ID : CVE-2022-31873**	N/A	H-TRE-TV-I-060722/330
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jun-22	6.1	Trendnet IP-110wn camera fw_tv-ip110wn_v2(1.2.2.68) has an xss vulnerability via the proname parameter in /admin/scheprofile.cgi **CVE ID : CVE-2022-31875**	N/A	H-TRE-TV-I-060722/331
Operating System					
Vendor: ABB					
Product: rex640_pcl1_firmware					
Incorrect Permission Assignment for Critical Resource	21-Jun-22	6.5	Incorrect Permission Assignment for Critical Resource vulnerability in ABB REX640 PCL1, REX640 PCL2, REX640 PCL3 allows an authenticated attacker to launch an attack against the user database file and	https://search.abb.com/library/Download.aspx?DocumentID=2NGA001421	O-ABB-REX6-060722/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			try to take control of an affected system node. **CVE ID : CVE-2022-1596**		
Product: rex640_pcl2_firmware					
Incorrect Permission Assignment for Critical Resource	21-Jun-22	6.5	Incorrect Permission Assignment for Critical Resource vulnerability in ABB REX640 PCL1, REX640 PCL2, REX640 PCL3 allows an authenticated attacker to launch an attack against the user database file and try to take control of an affected system node. **CVE ID : CVE-2022-1596**	https://search.abb.com/library/Download.aspx?DocumentID=2NGA001421	O-ABB-REX6-060722/333
Product: rex640_pcl3_firmware					
Incorrect Permission Assignment for Critical Resource	21-Jun-22	6.5	Incorrect Permission Assignment for Critical Resource vulnerability in ABB REX640 PCL1, REX640 PCL2, REX640 PCL3 allows an authenticated attacker to launch an attack against the user database file and try to take control of an affected system node. **CVE ID : CVE-2022-1596**	https://search.abb.com/library/Download.aspx?DocumentID=2NGA001421	O-ABB-REX6-060722/334
Vendor: anker					
Product: eufy_homebase_2_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	17-Jun-22	9.8	A use-after-free vulnerability exists in the mips_collector appsrv_server functionality of Anker Eufy Homebase 2 2.1.8.5h. A specially-crafted set of network packets can lead to remote code execution. The device is exposed to attacks from the network. **CVE ID : CVE-2022-21806**	N/A	O-ANK-EUFY-060722/335
Vendor: Apple					
Product: macos					
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30650**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-APP-MACO-060722/336
Out-of-bounds Read	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds read	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-APP-MACO-060722/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30651**		
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30652**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-APP-MACO-060722/338
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-APP-MACO-060722/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30653**		
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30654**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-APP-MACO-060722/340
Use After Free	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-APP-MACO-060722/341

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that a victim must open a malicious file. **CVE ID : CVE-2022-30655**		
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30656**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-APP-MACO-060722/342
Use After Free	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30657**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-APP-MACO-060722/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30658**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-APP-MACO-060722/344
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30659**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-APP-MACO-060722/345
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-APP-MACO-060722/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30660**		
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30661**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-APP-MACO-060722/347
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-APP-MACO-060722/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30662**		
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30663**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-APP-MACO-060722/349
Out-of-bounds Write	16-Jun-22	7.8	Adobe Animate version 22.0.5 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30664**	https://helpx.adobe.com/security/products/animate/apsb22-24.html	O-APP-MACO-060722/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30665**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-APP-MACO-060722/351
Vendor: Asus					
Product: rt-n53_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Jun-22	9.8	ASUS RT-N53 3.0.0.4.376.3754 has a command injection vulnerability in the SystemCmd parameter of the apply.cgi interface. **CVE ID : CVE-2022-31874**	N/A	O-ASU-RT-N-060722/352
Vendor: Cisco					
Product: ws-c2940-8tf-s_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-22	6.1	** Unsupported When Assigned ** Cisco Catalyst 2940 Series Switches provided by Cisco Systems, Inc. contain a reflected cross-site scripting vulnerability regarding error page generation. An	https://www.cisco.com/c/en/us/obsolete/switches/cisco-catalyst-2940-series-switches.html	O-CIS-WS-C-060722/353

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary script may be executed on the web browser of the user who is using the product. The affected firmware is prior to 12.2(50)SY released in 2011, and Cisco Catalyst 2940 Series Switches have been retired since January 2015. **CVE ID : CVE-2022-31734**		
Product: ws-c2940-8tt-s_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-22	6.1	** Unsupported When Assigned ** Cisco Catalyst 2940 Series Switches provided by Cisco Systems, Inc. contain a reflected cross-site scripting vulnerability regarding error page generation. An arbitrary script may be executed on the web browser of the user who is using the product. The affected firmware is prior to 12.2(50)SY released in 2011, and Cisco Catalyst 2940 Series Switches have been retired since January 2015. **CVE ID : CVE-2022-31734**	https://www.cisco.com/c/en/us/obsolete/switches/cisco-catalyst-2940-series-switches.html	O-CIS-WS-C-060722/354
Vendor: contec					
Product: sv-cpt-mc310_firmware					

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	6.1	SolarView Compact v6.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component Solar_AiConf.php. **CVE ID : CVE-2022-31373**	N/A	O-CON-SV-C-060722/355
Unrestricted Upload of File with Dangerous Type	21-Jun-22	9.8	An arbitrary file upload vulnerability /images/background/1.php in of SolarView Compact 6.0 allows attackers to execute arbitrary code via a crafted php file. **CVE ID : CVE-2022-31374**	N/A	O-CON-SV-C-060722/356
Vendor: Debian					
Product: debian_linux					
Buffer Over-read	20-Jun-22	7.8	Buffer Over-read in function grab_file_name in GitHub repository vim/vim prior to 8.2.4956. This vulnerability is capable of crashing the software, memory modification, and possible remote execution. **CVE ID : CVE-2022-1720**	https://github.com/vim/vim/commit/395bd1f6d3edc9f7edb5d1f2d7deaf5a9e3ab93c, https://huntr.dev/bounties/5ccfb386-7eb9-46e5-98e5-243ea4b358a8	O-DEB-DEBI-060722/357
Improper Neutralization of Special Elements	21-Jun-22	9.8	In addition to the c_rehash shell command injection identified in CVE-2022-1292, further	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=9639817da	O-DEB-DEBI-060722/358

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')		🟥	circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf	c8bbbaa64d09efad7464ccc405527c7, https://www.openssl.org/news/secadv/20220621.txt, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=7a9c027159fe9e1bbc2cd38a8a2914bff0d5abd9	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Affected 1.0.2-1.0.2ze). **CVE ID : CVE-2022-2068**		
Buffer Over-read	19-Jun-22	7.8	Buffer Over-read in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-2124**	https://github.com/vim/vim/commit/2f074f4685897ab7212e25931eeeb0212292829f, https://huntr.dev/bounties/8e9e056d-f733-4540-98b6-414bf36e0b42	O-DEB-DEBI-060722/359
Out-of-bounds Read	19-Jun-22	7.8	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2. **CVE ID : CVE-2022-2126**	https://github.com/vim/vim/commit/156d3911952d73b03d7420dc3540215247db0fe8, https://huntr.dev/bounties/8d196d9b-3d10-41d2-9f70-8ef0d08c946e	O-DEB-DEBI-060722/360
Vendor: Fedoraproject					
Product: fedora					
NULL Pointer Dereference	16-Jun-22	5.5	A NULL pointer dereference vulnerability was found in Ghostscript, which occurs when it tries to render a large number of bits in memory. When allocating a buffer device, it relies on an init_device_procs defined for the device	https://bugs.ghostscript.com/show_bug.cgi?id=704945, http://git.ghostscript.com/?p=ghostpdl.git;h=ae1061d948d88667bdf51d47d918c4684d0f67df, https://bugzill	O-FED-FEDO-060722/361

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that uses it as a prototype that depends upon the number of bits per pixel. For bpp > 64, mem_x_device is used and does not have an init_device_procs defined. This flaw allows an attacker to parse a large number of bits (more than 64 bits per pixel), which triggers a NULL pointer dereference flaw, causing an application to crash. **CVE ID : CVE-2022-2085**	a.redhat.com/show_bug.cgi?id=2095261	
Vendor: Fujitsu					
Product: eternus_cs8000_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jun-22	9.8	An issue was discovered on Fujitsu ETERNUS CentricStor CS8000 (Control Center) devices before 8.1A SP02 P04. The vulnerability resides in the requestTempFile function in hw_view.php. An attacker is able to influence the unitName POST parameter and inject special characters such as semicolons, backticks, or command-substitution sequences in order to force the application	https://support.ts.fujitsu.com/ProductSecurity/content/Fujitsu-PSIRT-PSS-IS-2022-050316-Security-Notice-SF.pdf	O-FUJ-ETER-060722/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands. **CVE ID : CVE-2022-31794**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jun-22	9.8	An issue was discovered on Fujitsu ETERNUS CentricStor CS8000 (Control Center) devices before 8.1A SP02 P04. The vulnerability resides in the grel_finfo function in grel.php. An attacker is able to influence the username (user), password (pw), and file-name (file) parameters and inject special characters such as semicolons, backticks, or command-substitution sequences in order to force the application to execute arbitrary commands. **CVE ID : CVE-2022-31795**	https://support.ts.fujitsu.com/ProductSecurity/content/Fujitsu-PSIRT-PSS-IS-2022-050316-Security-Notice-SF.pdf	O-FUJ-ETER-060722/363
Vendor: HP					
Product: hp-ux					
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system.	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218281	O-HP-HP-U-060722/364

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 218281. **CVE ID : CVE-2022-22317**		
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. **CVE ID : CVE-2022-22318**	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218283	O-HP-HP-U-060722/365
Vendor: IBM					
Product: aix					
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 218281. **CVE ID : CVE-2022-22317**	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218281	O-IBM-AIX-060722/366
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218283	O-IBM-AIX-060722/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impersonate another user on the system. **CVE ID : CVE-2022-22318**		
Improper Authentication	17-Jun-22	9.8	In some cases, an unsuccessful attempt to log into IBM Spectrum Protect Operations Center 8.1.0.000 through 8.1.14.000 does not cause the administrator's invalid sign-on count to be incremented on the IBM Spectrum Protect Server. An attacker could exploit this vulnerability using brute force techniques to gain unauthorized administrative access to the IBM Spectrum Protect Server. IBM X-Force ID: 226325. **CVE ID : CVE-2022-22485**	https://exchange.xforce.ibmcloud.com/vulnerabilities/226325, https://www.ibm.com/support/pages/node/6595655	O-IBM-AIX-060722/368
Product: z\/os					
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 218281.	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218281	O-IBM-Z\/O-060722/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22317		
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. **CVE ID : CVE-2022-22318**	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218283	O-IBM-Z\/O-060722/370
Vendor: Linux					
Product: linux_kernel					
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 218281. **CVE ID : CVE-2022-22317**	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218281	O-LIN-LINU-060722/371
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system.	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218283	O-LIN-LINU-060722/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22318		
Improper Authentication	17-Jun-22	9.8	In some cases, an unsuccessful attempt to log into IBM Spectrum Protect Operations Center 8.1.0.000 through 8.1.14.000 does not cause the administrator's invalid sign-on count to be incremented on the IBM Spectrum Protect Server. An attacker could exploit this vulnerability using brute force techniques to gain unauthorized administrative access to the IBM Spectrum Protect Server. IBM X-Force ID: 226325. **CVE ID : CVE-2022-22485**	https://exchange.xforce.ibmcloud.com/vulnerabilities/226325, https://www.ibm.com/support/pages/node/6595655	O-LIN-LINU-060722/373
Use After Free	18-Jun-22	3.3	drivers/block/floppy.c in the Linux kernel before 5.17.6 is vulnerable to a denial of service, because of a concurrency use-after-free flaw after deallocating raw_cmd in the raw_cmd_ioctl function. **CVE ID : CVE-2022-33981**	https://github.com/torvalds/linux/commit/233087ca063686964a53c829d547c7571e3f67bf, https://seclists.org/oss-sec/2022/q2/66, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17.6	O-LIN-LINU-060722/374

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Mercurycom					
Product: mipc451-4_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jun-22	8.8	MERCURY MIPC451-4 1.0.22 Build 220105 Rel.55642n was discovered to contain a remote code execution (RCE) vulnerability which is exploitable via a crafted POST request. **CVE ID : CVE-2022-31849**	N/A	O-MER-MIPC-060722/375
Vendor: mi					
Product: xiaomi_lamp_1_firmware					
Authentication Bypass by Capture-replay	16-Jun-22	8.8	Xiaomi Lamp 1 v2.0.4_0066 was discovered to be vulnerable to replay attacks. This allows attackers to to bypass the expected access restrictions and gain control of the switch and other functions via a crafted POST request. **CVE ID : CVE-2022-31277**	N/A	O-MI-XIAO-060722/376
Vendor: Microsoft					
Product: windows					
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system.	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218281	O-MIC-WIND-060722/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 218281. **CVE ID : CVE-2022-22317**		
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. **CVE ID : CVE-2022-22318**	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218283	O-MIC-WIND-060722/378
Exposure of Resource to Wrong Sphere	20-Jun-22	5.5	IBM Robotic Process Automation 21.0.2 could allow a local user to obtain sensitive web service configuration credentials from system memory. IBM X-Force ID: 223026. **CVE ID : CVE-2022-22414**	https://exchange.xforce.ibmcloud.com/vulnerabilities/223026, https://www.ibm.com/support/pages/node/6596071	O-MIC-WIND-060722/379
Improper Authentication	17-Jun-22	9.8	In some cases, an unsuccessful attempt to log into IBM Spectrum Protect Operations Center 8.1.0.000 through 8.1.14.000 does not cause the administrator's invalid sign-on count to be incremented on the IBM Spectrum Protect Server. An attacker could exploit this vulnerability	https://exchange.xforce.ibmcloud.com/vulnerabilities/226325, https://www.ibm.com/support/pages/node/6595655	O-MIC-WIND-060722/380

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using brute force techniques to gain unauthorized administrative access to the IBM Spectrum Protect Server. IBM X-Force ID: 226325. **CVE ID : CVE-2022-22485**		
Improper Privilege Management	21-Jun-22	8.8	AtlasVPN - Privilege Escalation Lack of proper security controls on named pipe messages can allow an attacker with low privileges to send a malicious payload and gain SYSTEM permissions on a windows computer where the AtlasVPN client is installed. **CVE ID : CVE-2022-23171**	N/A	O-MIC-WIND-060722/381
Exposure of Resource to Wrong Sphere	17-Jun-22	6.5	IBM Robotic Process Automation 20.10.0, 20.12.5, 21.0.0, 21.0.1, and 21.0.2 contains a vulnerability that could allow a user to obtain sensitive information due to information properly masked in the control center UI. IBM X-Force ID: 227294. **CVE ID : CVE-2022-30607**	https://www.ibm.com/support/pages/node/6595759, https://exchange.xforce.ibmcloud.com/vulnerabilities/227294	O-MIC-WIND-060722/382
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1	https://helpx.adobe.com/security/products/i	O-MIC-WIND-060722/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30650**	ncopy/apsb22-29.html	
Out-of-bounds Read	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30651**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-MIC-WIND-060722/384
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are	https://helpx.adobe.com/security/products/i	O-MIC-WIND-060722/385

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30652**	ncopy/apsb22-29.html	
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30653**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-MIC-WIND-060722/386
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-MIC-WIND-060722/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30654**		
Use After Free	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30655**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-MIC-WIND-060722/388
Out-of-bounds Write	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-MIC-WIND-060722/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30656		
Use After Free	16-Jun-22	7.8	Adobe InCopy versions 17.2 (and earlier) and 16.4.1 (and earlier) are affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30657**	https://helpx.adobe.com/security/products/incopy/apsb22-29.html	O-MIC-WIND-060722/390
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30658**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-MIC-WIND-060722/391
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1	https://helpx.adobe.com/security/products/i	O-MIC-WIND-060722/392

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30659**	ndesign/apsb22-30.html	
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30660**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-MIC-WIND-060722/393
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-MIC-WIND-060722/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30661**		
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30662**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-MIC-WIND-060722/395
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-MIC-WIND-060722/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that a victim must open a malicious file. **CVE ID : CVE-2022-30663**		
Out-of-bounds Write	16-Jun-22	7.8	Adobe Animate version 22.0.5 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30664**	https://helpx.adobe.com/security/products/animate/apsb22-24.html	O-MIC-WIND-060722/397
Out-of-bounds Write	16-Jun-22	7.8	Adobe InDesign versions 17.2.1 (and earlier) and 16.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30665**	https://helpx.adobe.com/security/products/indesign/apsb22-30.html	O-MIC-WIND-060722/398
Improper Authorization	16-Jun-22	8.8	RoboHelp Server earlier versions than RHS 11 Update 3 are affected by an	https://helpx.adobe.com/security/products/robohelp-	O-MIC-WIND-060722/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	Improper Authorization vulnerability which could lead to privilege escalation. An authenticated attacker could leverage this vulnerability to achieve full administrator privileges. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2022-30670**	server/apsb22-31.html	
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	17-Jun-22	5.5	paymentrequest.py in Electrum before 4.2.2 allows a file:// URL in the r parameter of a payment request (e.g., within QR code data). On Windows, this can lead to capture of credentials over SMB. On Linux and UNIX, it can lead to a denial of service by specifying the /dev/zero filename. **CVE ID : CVE-2022-31246**	N/A	O-MIC-WIND-060722/400
N/A	23-Jun-22	9.8	The function that calls the diff tool in Diffy 3.4.1 does not properly handle double quotes in a filename when run in a windows environment. This allows attackers to execute arbitrary	https://github.com/samg/diffy/commit/478f392082b66d38f54a02b4bb9c41be32fd6593	O-MIC-WIND-060722/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted string. **CVE ID : CVE-2022-33127**		
Vendor: Netgear					
Product: wnap320_firmware					
Incorrect Authorization	17-Jun-22	5.3	netgear wnap320 router WNAP320_V2.0.3_firmware is vulnerable to Incorrect Access Control via /recreate.php, which can leak all users cookies. **CVE ID : CVE-2022-31876**	https://www.netgear.com/about/security/	O-NET-WNAP-060722/402
Vendor: Nuuo					
Product: nvrsolo_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-22	6.1	NUUO Network Video Recorder NVRsolo v03.06.02 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via login.php. **CVE ID : CVE-2022-33119**	N/A	O-NUU-NVRS-060722/403
Vendor: Oracle					
Product: solaris					
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218281	O-ORA-SOLA-060722/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the system. IBM X-Force ID: 218281. **CVE ID : CVE-2022-22317**		
Insufficient Session Expiration	20-Jun-22	9.8	IBM Curam Social Program Management 8.0.0 and 8.0.1 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. **CVE ID : CVE-2022-22318**	https://www.ibm.com/support/pages/node/6596049, https://exchange.xforce.ibmcloud.com/vulnerabilities/218283	O-ORA-SOLA-060722/405
Vendor: Phoenixcontact					
Product: axc_1050_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-AXC_-060722/406
Product: axc_1050_xc_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device.	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-AXC_-060722/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31800		
Product: axc_3050_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-AXC_-060722/408
Product: fc_350_pci_eth_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-FC_3-060722/409
Product: ilc1x0_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-ILC1-060722/410
Product: ilc1x1_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-ILC1-060722/411
Product: ilc_1x1_gsm\/gprs_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-ILC_-060722/412
Product: ilc_3xx_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-ILC_-060722/413
Product: pc_worx_rt_basic_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-PC_W-060722/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**		
Product: pc_worx_srt_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-PC_W-060722/415
Product: proconos					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to the devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31801**	https://cert.vde.com/en/advisories/VDE-2022-026/	O-PHO-PROC-060722/416
Product: rfc_430_eth-ib_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device.	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-RFC_-060722/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31800		
Product: rfc_450_eth-ib_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-RFC_-060722/418
Product: rfc_460r_pn_3tx-s_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-RFC_-060722/419
Product: rfc_460r_pn_3tx_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-RFC_-060722/420
Product: rfc_470s_pn_3tx_firmware					

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-RFC_-060722/421
Product: rfc_470_pn_3tx_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-RFC_-060722/422
Product: rfc_480s_pn_4tx_firmware					
Insufficient Verification of Data Authenticity	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to devices based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31800**	https://cert.vde.com/en/advisories/VDE-2022-025/	O-PHO-RFC_-060722/423
Vendor: phoenixcontact-software					
Product: proconos_eclr					
Insufficient Verification of Data	21-Jun-22	9.8	An unauthenticated, remote attacker could upload malicious logic to the devices	https://cert.vde.com/en/advi	O-PHO-PROC-060722/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			based on ProConOS/ProConOS eCLR in order to gain full control over the device. **CVE ID : CVE-2022-31801**	sories/VDE-2022-026/	
Vendor: quectel					
Product: rg502q-ea_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Jun-22	9.8	The Quectel RG502Q-EA modem before 2022-02-23 allow OS Command Injection. **CVE ID : CVE-2022-26147**	N/A	O-QUE-RG50-060722/425
Vendor: Redhat					
Product: enterprise_linux					
N/A	21-Jun-22	8.8	A set of pre-production kernel packages of Red Hat Enterprise Linux for IBM Power architecture can be booted by the grub in Secure Boot mode even though it shouldn't. These kernel builds don't have the secure boot lockdown patches applied to it and can bypass the secure boot validations, allowing the attacker to load another non-trusted code.	https://bugzilla.redhat.com/show_bug.cgi?id=2089529	O-RED-ENTE-060722/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1665		
Vendor: Tenda					
Product: hg9_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jun-22	8.8	Tenda ONT GPON AC1200 Dual band WiFi HG9 v1.0.1 is vulnerable to Command Injection via the Ping function. **CVE ID : CVE-2022-30023**	N/A	O-TEN-HG9_-060722/427
Vendor: Trendnet					
Product: tew-831dr_firmware					
Weak Password Requirements	16-Jun-22	8.8	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The default pre-shared key for the Wi-Fi networks is the same for every router except for the last four digits. The device default pre-shared key for both 2.4 GHz and 5 GHz networks can be guessed or brute-forced by an attacker within range of the Wi-Fi network. **CVE ID : CVE-2022-30325**	N/A	O-TRE-TEW--060722/428
Improper Neutralization of Input During	16-Jun-22	5.4	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The network	N/A	O-TRE-TEW--060722/429

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			pre-shared key field on the web interface is vulnerable to XSS. An attacker can use a simple XSS payload to crash the basic.config page of the web interface. **CVE ID : CVE-2022-30326**		
Cross-Site Request Forgery (CSRF)	16-Jun-22	6.5	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The web interface is vulnerable to CSRF. An attacker can change the pre-shared key of the Wi-Fi router if the interface's IP address is known. **CVE ID : CVE-2022-30327**	N/A	O-TRE-TEW--060722/430
Cross-Site Request Forgery (CSRF)	16-Jun-22	6.5	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The username and password setup for the web interface does not require entering the existing password. A malicious user can change the username and password of the interface. **CVE ID : CVE-2022-30328**	N/A	O-TRE-TEW--060722/431

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	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Jun-22	9.8	An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. An OS injection vulnerability exists within the web interface, allowing an attacker with valid credentials to execute arbitrary shell commands. **CVE ID : CVE-2022-30329**	N/A	O-TRE-TEW--060722/432
Product: tv-ip110wn_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jun-22	6.1	Trendnet IP-110wn camera fw_tv-ip110wn_v2(1.2.2.68) has an XSS vulnerability via the prefix parameter in /admin/general.cgi. **CVE ID : CVE-2022-31873**	N/A	O-TRE-TV-I-060722/433
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jun-22	6.1	Trendnet IP-110wn camera fw_tv-ip110wn_v2(1.2.2.68) has an xss vulnerability via the proname parameter in /admin/scheprofile.cgi **CVE ID : CVE-2022-31875**	N/A	O-TRE-TV-I-060722/434