National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 - 30 Nov 2023 Vol. 10 No. 22

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 10web					
Product: 10web_booster					
Affected Version(s): * Up to (excluding) 2.24.18					
N/A	27-Nov-2023	9.1	The 10Web Booster WordPress plugin before 2.24.18 does not validate the option name given to some AJAX actions, allowing unauthenticated users to delete arbitrary options from the database, leading to denial of service. **CVE ID : CVE-2023-5559**	N/A	A-10W-10WE-181223/1
Product: seo					
Affected Version(s): * Up to (including) 1.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in 10Web SEO by 10Web plugin <= 1.2.9 versions. **CVE ID : CVE-2023-34375**	N/A	A-10W-SEO-181223/2
Vendor: accesspressthemes					
Product: social_auto_poster					
Affected Version(s): * Up to (including) 2.1.4					
N/A	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in AccessPress Themes Social Auto	N/A	A-ACC-SOCI-181223/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Poster plugin <= 2.1.4 versions. **CVE ID : CVE-2023-26532**		
Vendor: acurax					
Product: under_construction_\/_maintenance_mode					
Affected Version(s): * Up to (including) 2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Acurax Under Construction / Maintenance Mode from Acurax plugin <= 2.6 versions. **CVE ID : CVE-2023-39926**	N/A	A-ACU-UNDE-181223/4
Vendor: Admidio					
Product: admidio					
Affected Version(s): 4.2.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	6.1	Admidio v4.2.12 and below is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-47380**	https://www.getastra.com/blog/security-audit/reflected-xss-vulnerability-in-admidio/	A-ADM-ADMI-181223/5
Vendor: Adobe					
Product: acrobat					
Affected Version(s): From (including) 20.001.30005 Up to (including) 20.005.30539					
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free	N/A	A-ADO-ACRO-181223/6

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
			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-2023-44336**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44337**	N/A	A-ADO-ACRO-181223/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44338**	N/A	A-ADO-ACRO-181223/8
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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	N/A	A-ADO-ACRO-181223/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44359**		
Access of Uninitialized Pointer	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-44365**	N/A	A-ADO-ACRO-181223/10
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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	N/A	A-ADO-ACRO-181223/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44366**		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44367**	N/A	A-ADO-ACRO-181223/12
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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	N/A	A-ADO-ACRO-181223/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-44371**		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44372**	N/A	A-ADO-ACRO-181223/14
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	N/A	A-ADO-ACRO-181223/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44340**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44348**	N/A	A-ADO-ACRO-181223/16
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	N/A	A-ADO-ACRO-181223/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44356**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44357**	N/A	A-ADO-ACRO-181223/18
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that	N/A	A-ADO-ACRO-181223/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44358**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44360**	N/A	A-ADO-ACRO-181223/20
Use After Free	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and	N/A	A-ADO-ACRO-181223/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.005.30524 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44361**		
Out-of-bounds Read	16-Nov-2023	5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44339**	N/A	A-ADO-ACRO-181223/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: acrobat_dc					
Affected Version(s): From (including) 15.008.20082 Up to (excluding) 23.006.20380					
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44336**	N/A	A-ADO-ACRO-181223/23
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	N/A	A-ADO-ACRO-181223/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44337**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44338**	N/A	A-ADO-ACRO-181223/25
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free vulnerability that	N/A	A-ADO-ACRO-181223/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-44359**		
Access of Uninitialized Pointer	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-44365**	N/A	A-ADO-ACRO-181223/27
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds write vulnerability that	N/A	A-ADO-ACRO-181223/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-44366**		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44367**	N/A	A-ADO-ACRO-181223/29
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the	N/A	A-ADO-ACRO-181223/30

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-2023-44371**		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44372**	N/A	A-ADO-ACRO-181223/31
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	N/A	A-ADO-ACRO-181223/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44340**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44348**	N/A	A-ADO-ACRO-181223/33
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that	N/A	A-ADO-ACRO-181223/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44356**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44357**	N/A	A-ADO-ACRO-181223/35
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and	N/A	A-ADO-ACRO-181223/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44358**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	A-ADO-ACRO-181223/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-44360		
Use After Free	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44361**	N/A	A-ADO-ACRO-181223/38
Out-of-bounds Read	16-Nov-2023	5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this	N/A	A-ADO-ACRO-181223/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44339**		
Product: acrobat_reader					
Affected Version(s): From (including) 20.001.30005 Up to (excluding) 20.005.30539					
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44336**	N/A	A-ADO-ACRO-181223/40
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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	N/A	A-ADO-ACRO-181223/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-44337**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44338**	N/A	A-ADO-ACRO-181223/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44359**	N/A	A-ADO-ACRO-181223/43
Access of Uninitialized Pointer	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-44365**	N/A	A-ADO-ACRO-181223/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44366**	N/A	A-ADO-ACRO-181223/45
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44367**	N/A	A-ADO-ACRO-181223/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44371**	N/A	A-ADO-ACRO-181223/47
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44372**	N/A	A-ADO-ACRO-181223/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44340**	N/A	A-ADO-ACRO-181223/49
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	N/A	A-ADO-ACRO-181223/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44348**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44356**	N/A	A-ADO-ACRO-181223/51
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	N/A	A-ADO-ACRO-181223/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44357**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44358**	N/A	A-ADO-ACRO-181223/53
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that	N/A	A-ADO-ACRO-181223/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44360**		
Use After Free	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44361**	N/A	A-ADO-ACRO-181223/55
Out-of-bounds Read	16-Nov-2023	5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and	N/A	A-ADO-ACRO-181223/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44339**		
Product: acrobat_reader_dc					
Affected Version(s): From (including) 15.008.20082 Up to (excluding) 23.006.20380					
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44336**	N/A	A-ADO-ACRO-181223/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44337**	N/A	A-ADO-ACRO-181223/58
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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	N/A	A-ADO-ACRO-181223/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-44338**		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44359**	N/A	A-ADO-ACRO-181223/60
Access of Uninitialized Pointer	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that	N/A	A-ADO-ACRO-181223/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-44365**		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44366**	N/A	A-ADO-ACRO-181223/62
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code	N/A	A-ADO-ACRO-181223/63

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-2023-44367**		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44371**	N/A	A-ADO-ACRO-181223/64
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user.	N/A	A-ADO-ACRO-181223/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44372**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44340**	N/A	A-ADO-ACRO-181223/66
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory.	N/A	A-ADO-ACRO-181223/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44348**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44356**	N/A	A-ADO-ACRO-181223/68
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-	N/A	A-ADO-ACRO-181223/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44357**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44358**	N/A	A-ADO-ACRO-181223/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44360**	N/A	A-ADO-ACRO-181223/71
Use After Free	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	N/A	A-ADO-ACRO-181223/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-44361**		
Out-of-bounds Read	16-Nov-2023	5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44339**	N/A	A-ADO-ACRO-181223/73
Product: after_effects					
Affected Version(s): From (including) 23.0 Up to (including) 23.6					
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47066**		
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47067**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47068**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/76
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/77

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-2023-47069**		
Out-of-bounds Write	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47070**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/78
Out-of-bounds Write	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-47073**		
Out-of-bounds Read	17-Nov-2023	5.5	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47071**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/80
Access of Uninitialized Pointer	17-Nov-2023	3.3	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47072**		
Affected Version(s): From (including) 24.0 Up to (excluding) 24.0.2					
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47066**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/82
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47067**		
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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.	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47068		
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47069**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/85
Out-of-bounds Write	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-47070**		
Out-of-bounds Write	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47073**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/87
Out-of-bounds Read	17-Nov-2023	5.5	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-47071**		
Access of Uninitialized Pointer	17-Nov-2023	3.3	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47072**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	A-ADO-AFTE-181223/89
Product: animate					
Affected Version(s): * Up to (including) 23.0.2					
Out-of-bounds Read	17-Nov-2023	5.5	Adobe Animate versions 23.0.2 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/animate/apsb23-61.html	A-ADO-ANIM-181223/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44325**		
Product: audition					
Affected Version(s): * Up to (including) 23.6.1					
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47046**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/91
Access of Uninitialized Pointer	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/92

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-2023-47047**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47048**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/93
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47049**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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.	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47050		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47051**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/96
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47052		
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47053**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/98
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47054**		
Affected Version(s): 24.0					
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47046**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/100
Access of Uninitialized Pointer	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47047**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47048**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/102
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47049**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47050**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47051**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/105
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47052**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47053**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/107
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/audition/apsb23-64.html	A-ADO-AUDI-181223/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47054**		
Product: bridge					
Affected Version(s): * Up to (including) 13.0.4					
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44327**	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	A-ADO-BRID-181223/109
Use After Free	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	A-ADO-BRID-181223/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44328**		
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44329**	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	A-ADO-BRID-181223/111
Affected Version(s): 14.0.0					
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by an Access of	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	A-ADO-BRID-181223/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44327**		
Use After Free	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44328**	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	A-ADO-BRID-181223/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44329**	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	A-ADO-BRID-181223/114
Product: coldfusion					
Affected Version(s): * Up to (excluding) 2021					
Deserialization of Untrusted Data	17-Nov-2023	9.8	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-44350		
Deserialization of Untrusted Data	17-Nov-2023	9.8	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-44351**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/116
Deserialization of Untrusted Data	17-Nov-2023	9.8	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-44353**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/117
Improper Access Control	17-Nov-2023	7.5	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and	https://helpx.adobe.com/security/products/c	A-ADO-COLD-181223/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An unauthenticated attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-26347**	oldfusion/apsb23-52.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-2023	6.1	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an unauthenticated attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-44352**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-2023	4.3	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An unauthenticated attacker could leverage this vulnerability to impact a minor integrity feature. Exploitation of this issue does require user interaction. **CVE ID : CVE-2023-44355**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/120
Affected Version(s): 2021					
Deserialization of Untrusted Data	17-Nov-2023	9.8	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-44350**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	17-Nov-2023	9.8	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-44351**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/122
Deserialization of Untrusted Data	17-Nov-2023	9.8	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-44353**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/123
Improper Access Control	17-Nov-2023	7.5	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Improper Access Control	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in a Security feature bypass. An unauthenticated attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-26347**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-2023	6.1	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an unauthenticated attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-44352**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-2023	4.3	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An unauthenticated attacker could leverage this vulnerability to impact a minor integrity feature. Exploitation of this issue does require user interaction. **CVE ID : CVE-2023-44355**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/126
Affected Version(s): 2023					
Deserialization of Untrusted Data	17-Nov-2023	9.8	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-44350**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	17-Nov-2023	9.8	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-44351**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/128
Deserialization of Untrusted Data	17-Nov-2023	9.8	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-44353**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/129
Improper Access Control	17-Nov-2023	7.5	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Improper Access Control	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in a Security feature bypass. An unauthenticated attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-26347**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-2023	6.1	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an unauthenticated attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-44352**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Nov-2023	4.3	Adobe ColdFusion versions 2023.5 (and earlier) and 2021.11 (and earlier) are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An unauthenticated attacker could leverage this vulnerability to impact a minor integrity feature. Exploitation of this issue does require user interaction. **CVE ID : CVE-2023-44355**	https://helpx.adobe.com/security/products/coldfusion/apsb23-52.html	A-ADO-COLD-181223/132
Product: css-tools					
Affected Version(s): * Up to (excluding) 4.3.1					
N/A	17-Nov-2023	5.3	@adobe/css-tools version 4.3.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a minor denial of service while attempting to parse CSS. Exploitation of this issue does not require user interaction or privileges. **CVE ID : CVE-2023-26364**	https://github.com/adobe/css-tools/security/advisories/GHSA-hpx4-r86g-5jrg	A-ADO-CSS--181223/133
Product: dimension					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 3.4.9					
Out-of-bounds Read	17-Nov-2023	5.5	Adobe Dimension versions 3.4.9 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44326**	https://helpx.adobe.com/security/products/dimension/apsb23-62.html	A-ADO-DIME-181223/134
Product: framemaker					
Affected Version(s): * Up to (including) 2022					
Improper Authentication	17-Nov-2023	9.8	Adobe FrameMaker versions 2022 and earlier are affected by an Improper Authentication vulnerability that could result in a Security feature bypass. An unauthenticated attacker can abuse this vulnerability to access the API and leak default admin's password. Exploitation of this issue does not	https://helpx.adobe.com/security/products/framemaker/apsb23-58.html	A-ADO-FRAM-181223/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			require user interaction. **CVE ID : CVE-2023-44324**		
Product: incopy					
Affected Version(s): * Up to (including) 17.04.2					
Out-of-bounds Read	16-Nov-2023	7.8	Adobe InCopy versions 18.5 (and earlier) and 17.4.2 (and earlier) are affected by 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-2023-26368**	https://helpx.adobe.com/security/products/incopy/apsb23-60.html	A-ADO-INCO-181223/136
Affected Version(s): From (including) 18.0 Up to (including) 18.5					
Out-of-bounds Read	16-Nov-2023	7.8	Adobe InCopy versions 18.5 (and earlier) and 17.4.2 (and earlier) are affected by are affected by an out-of-bounds read vulnerability when	https://helpx.adobe.com/security/products/incopy/apsb23-60.html	A-ADO-INCO-181223/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-26368**		
Product: media_encoder					
Affected Version(s): * Up to (including) 23.6.0					
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	A-ADO-MEDI-181223/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47040**		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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-2023-47041**	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	A-ADO-MEDI-181223/139
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	A-ADO-MEDI-181223/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-47042**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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-2023-47043**	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	A-ADO-MEDI-181223/141
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory.	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	A-ADO-MEDI-181223/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47044**		
Affected Version(s): From (including) 24.0.0 Up to (including) 24.0.2					
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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-2023-47040**	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	A-ADO-MEDI-181223/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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-2023-47041**	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	A-ADO-MEDI-181223/144
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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-2023-47042**	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	A-ADO-MEDI-181223/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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-2023-47043**	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	A-ADO-MEDI-181223/146
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	A-ADO-MEDI-181223/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47044**		
Product: photoshop					
Affected Version(s): * Up to (including) 24.7.1					
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (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-2023-44330**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/148
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44331**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44333**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/150
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an	https://helpx.adobe.com/security/products/	A-ADO-PHOT-181223/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44334**	photoshop/apsb23-56.html	
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44335**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/152
Affected Version(s): * Up to (including) 24.7.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44332**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/153
Affected Version(s): * Up to (including) 25.0					
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (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	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44330**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44331**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/155
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44333**		
Affected Version(s): * Up to (including) 25.1					
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44332**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/157
Affected Version(s): 25.0					
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44334**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44335**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	A-ADO-PHOT-181223/159
Product: premiere_pro					
Affected Version(s): 24.0					
Use After Free	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by a Use After Free vulnerability that	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47055**		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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-2023-47056**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/161
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47057**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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-2023-47058**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/163
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47059**		
Access of Uninitialized Pointer	16-Nov-2023	3.3	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47060**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/165
Affected Version(s): * Up to (including) 23.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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-2023-47055**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/166
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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-2023-47056**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/167
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier)	https://helpx.adobe.com/security/products/	A-ADO-PREM-181223/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47057**	premiere_pro/apsb23-65.html	
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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-2023-47058**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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-2023-47059**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/170
Access of Uninitialized Pointer	16-Nov-2023	3.3	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	A-ADO-PREM-181223/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47060**		
Product: robohelp_server					
Affected Version(s): * Up to (including) 11.4					
Improper Input Validation	17-Nov-2023	7.5	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Input Validation vulnerability that could lead to information disclosure by an unauthenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-22272**	https://helpx.adobe.com/security/products/robohelp-server/apsb23-53.html	A-ADO-ROBO-181223/172
Improper Restriction of XML External Entity Reference	17-Nov-2023	7.5	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could lead to information disclosure by an unauthenticated attacker. Exploitation of this	https://helpx.adobe.com/security/products/robohelp-server/apsb23-53.html	A-ADO-ROBO-181223/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction. **CVE ID : CVE-2023-22274**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Nov-2023	7.5	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead to information disclosure by an unauthenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-22275**	https://helpx.adobe.com/security/products/robohelp-server/apsb23-53.html	A-ADO-ROBO-181223/174
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Nov-2023	7.2	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to Remote Code Execution by an admin authenticated	https://helpx.adobe.com/security/products/robohelp-server/apsb23-53.html	A-ADO-ROBO-181223/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-22273**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Nov-2023	6.5	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead to information disclosure by an low-privileged authenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-22268**	https://helpx.adobe.com/security/products/robohelp-server/apsb23-53.html	A-ADO-ROBO-181223/176
Vendor: alexufo					
Product: youtube_speedload					
Affected Version(s): * Up to (including) 0.6.3					
Cross-Site Request Forgery (CSRF)	16-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Alexufo Youtube SpeedLoad plugin <= 0.6.3 versions. **CVE ID : CVE-2023-47688**	N/A	A-ALE-YOUT-181223/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: allurewebsolutions					
Product: wp_post_popup					
Affected Version(s): * Up to (including) 3.7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	4.8	The WP Post Popup WordPress plugin through 3.7.3 does not sanitise and escape some of its inputs, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-4808**	N/A	A-ALL-WP_P-181223/178
Vendor: Apache					
Product: storm					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.6.0					
N/A	23-Nov-2023	5.5	On unix-like systems, the temporary directory is shared between all user. As such, writing to this directory using APIs that do not explicitly set the file/directory permissions can lead to information disclosure. Of note, this does not impact modern	https://lists.apache.org/thread/88oc1vqfjtr29cz5xts0v2wm5pmhbm0l	A-APA-STOR-181223/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MacOS Operating Systems. The method File.createTempFile on unix-like systems creates a file with predefined name (so easily identifiable) and by default will create this file with the permissions -rw-r--r--. Thus, if sensitive information is written to this file, other local users can read this information. File.createTempFile(String, String) will create a temporary file in the system temporary directory if the 'java.io.tmpdir' system property is not explicitly set. This affects the class https://github.com/apache/storm/blob/master/storm-core/src/jvm/org/apache/storm/utils/TopologySpoutLag.java#L99 and was introduced by https://issues.a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pache.org/jira/browse/STORM-3123 In practice, this has a very limited impact as this class is used only if ui.disable.spout.lag.monitoring is set to false, but its value is true by default. Moreover, the temporary file gets deleted soon after its creation. The solution is to use Files.createTempFile https://docs.oracle.com/en/java/javase/11/docs/api/java.base/java/nio/file/Files.html#createTempFile(java.lang.String,java.lang.String,java.nio.file.attribute.FileAttribute...) instead. We recommend that all users upgrade to the latest version of Apache Storm. **CVE ID : CVE-2023-43123**		
Product: submarine					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 0.7.0 Up to (excluding) 0.8.0					
N/A	22-Nov-2023	9.8	Apache Software Foundation Apache Submarine has an SQL injection vulnerability when a user logs in. This issue can result in unauthorized login. Now we have fixed this issue and now user must have the correct login to access workbench. This issue affects Apache Submarine: from 0.7.0 before 0.8.0. We recommend that all submarine users with 0.7.0 upgrade to 0.8.0, which not only fixes the issue, supports the oidc authentication mode, but also removes the case of unauthenticated logins. If using the version lower than 0.8.0 and not want to upgrade, you can try cherry-pick PR https://github.com/apache/submarine/pull/1037 https://github.com/apache/submarine/pull/1054 and rebuild the	https://issues.apache.org/jira/browse/SUBMARINE-1361, https://lists.apache.org/thread/g99h773vd49n1wyghdq1llv2f83w1b3r	A-APA-SUBM-181223/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			submarine-server image to fix this. **CVE ID : CVE-2023-37924**		
N/A	20-Nov-2023	9.8	Apache Software Foundation Apache Submarine has a bug when serializing against yaml. The bug is caused by snakeyaml https://nvd.nist.gov/vuln/detail/CVE-2022-1471 . Apache Submarine uses JAXRS to define REST endpoints. In order to handle YAML requests (using application/yaml content-type), it defines a YamlEntityProvider entity provider that will process all incoming YAML requests. In order to unmarshal the request, the readFrom method is invoked, passing the entityStream containing the user-supplied data	https://github.com/apache/submarine/pull/1054	A-APA-SUBM-181223/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	in `submarine-server/server-core/src/main/java/org/apache/submarine/server/utils/YamlUtils.java`. We have now fixed this issue in the new version by replacing to `jackson-dataformat-yaml`. This issue affects Apache Submarine: from 0.7.0 before 0.8.0. Users are recommended to upgrade to version 0.8.0, which fixes this issue. If using the version smaller than 0.8.0 and not want to upgrade, you can try cherry-pick PR https://github.com/apache/submarine/pull/1054 and rebuild the submart-server image to fix this. **CVE ID : CVE-2023-46302**		
Product: superset					
Affected Version(s): * Up to (excluding) 2.1.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	27-Nov-2023	8.8	Improper authorization check and possible privilege escalation on Apache Superset up to but excluding 2.1.2. Using the default examples database connection that allows access to both the examples schema and Apache Superset's metadata database, an attacker using a specially crafted CTE SQL statement could change data on the metadata database. This weakness could result on tampering with the authentication/authorization data. **CVE ID : CVE-2023-40610**	https://lists.apache.org/thread/jvgxpk4dbxyqtsgtl4pdgbd520rc0rot	A-APA-SUPE-181223/182
Vendor: apppresser					
Product: apppresser					
Affected Version(s): * Up to (excluding) 4.3.0					
Weak Password Recovery Mechanism for Forgotten Password	18-Nov-2023	9.8	The AppPresser plugin for WordPress is vulnerable to unauthorized password resets in versions up to, and including 4.2.5. This is due to the	https://plugins.trac.wordpress.org/changeset/2997160/apppresser	A-APP-APPP-181223/183

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
			plugin generating too weak a reset code, and the code used to reset the password has no attempt or time limit. **CVE ID : CVE-2023-4214**		
Vendor: archerydms					
Product: archery					
Affected Version(s): 1.9.0					
Use of Hard-coded Credentials	16-Nov-2023	7.5	Archery v1.10.0 uses a non-random or static IV for Cipher Block Chaining (CBC) mode in AES encryption. This vulnerability can lead to the disclosure of information and communications. **CVE ID : CVE-2023-48053**	N/A	A-ARC-ARCH-181223/184
Vendor: ari-soft					
Product: ari_stream_quiz					
Affected Version(s): * Up to (including) 1.2.32					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ARI Soft ARI Stream Quiz – WordPress Quizzes Builder	N/A	A-ARI-ARI_-181223/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin <= 1.2.32 versions. **CVE ID : CVE-2023-47835**		
Vendor: armanidrisi					
Product: dev_blog					
Affected Version(s): 1.0					
N/A	21-Nov-2023	5.4	Dev blog v1.0 allows to exploit an XSS through an unrestricted file upload, together with a bad entropy of filenames. With this an attacker can upload a malicious HTML file, then guess the filename of the uploaded file and send it to a potential victim. **CVE ID : CVE-2023-6142**	N/A	A-ARM-DEV_-181223/186
N/A	21-Nov-2023	4.8	Dev blog v1.0 allows to exploit an account takeover through the "user" cookie. With this, an attacker can access any user's session just by knowing their username. **CVE ID : CVE-2023-6144**	N/A	A-ARM-DEV_-181223/187
Vendor: Artica					
Product: pandora_fms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 700 Up to (excluding) 773					
Insertion of Sensitive Information into Log File	23-Nov-2023	9.8	Cron log backup files contain administrator session IDs. It is trivial for any attacker who can reach the Pandora FMS Console to scrape the cron logs directory for cron log backups. The contents of these log files can then be abused to authenticate to the application as an administrator. This issue affects Pandora FMS <= 772. **CVE ID : CVE-2023-4677**	https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/188
Uncontrolled Search Path Element	23-Nov-2023	7.5	Uncontrolled Search Path Element vulnerability in Pandora FMS on all allows Leveraging/Manipulating Configuration File Search Paths. This vulnerability allows access to files with sensitive information. This issue affects Pandora FMS: from 700 through 772. **CVE ID : CVE-2023-41787**	https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	23-Nov-2023	6.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Pandora FMS on all allows File Discovery. This vulnerability allows users with low privileges to download database backups. This issue affects Pandora FMS: from 700 through 772. **CVE ID : CVE-2023-41786**	https://https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/190
Affected Version(s): From (including) 700 Up to (excluding) 774					
Unrestricted Upload of File with Dangerous Type	23-Nov-2023	8.8	Unrestricted Upload of File with Dangerous Type vulnerability in Pandora FMS on all allows Accessing Functionality Not Properly Constrained by ACLs. This vulnerability allows attackers to execute code via PHP file uploads. This issue affects Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41788**	https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/191
Unrestricted Upload of File with	23-Nov-2023	8.8	Unrestricted Upload of File with Dangerous Type vulnerability in	https://pandorafms.com/en/security/common-	A-ART-PAND-181223/192

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			Pandora FMS on all allows Accessing Functionality Not Properly Constrained by ACLs. This vulnerability allowed PHP executable files to be uploaded through the file manager. This issue affects Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41812**	vulnerabilities-and-exposures/	
Affected Version(s): From (including) 700 Up to (including) 773					
Uncontrolled Search Path Element	23-Nov-2023	9.8	Uncontrolled Search Path Element vulnerability in Pandora FMS on all allows Leveraging/Manipulating Configuration File Search Paths. This vulnerability allows to access the server configuration file and to compromise the database. This issue affects Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41790**	https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/193
N/A	23-Nov-2023	8.8	Improper Privilege Management vulnerability in Pandora FMS on all	https://pandorafms.com/en/security/common-	A-ART-PAND-181223/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows Privilege Escalation. This vulnerability allows a user to escalate permissions on the system shell. This issue affects Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41807**	vulnerabilities-and-exposures/	
N/A	23-Nov-2023	7.5	Improper Privilege Management vulnerability in Pandora FMS on all allows Privilege Escalation. This vulnerability causes that a bad privilege assignment could cause a DOS attack that affects the availability of the Pandora FMS server. This issue affects Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41806**	https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/195
N/A	23-Nov-2023	7.5	Improper Privilege Management vulnerability in Pandora FMS on all allows Privilege Escalation. This vulnerability allows an unauthorised user to escalate and read sensitive files as if they were root. This issue affects	https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41808**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). This vulnerability allows an attacker to perform cookie hijacking and log in as that user without the need for credentials. This issue affects Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41789**	https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/197
Cross-Site Request Forgery (CSRF)	23-Nov-2023	6.1	Cross-Site Request Forgery (CSRF) vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). This vulnerability allowed Javascript code to be executed in the SNMP Trap Editor. This issue affects Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41792**	https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). This vulnerability allowed Javascript code to be executed in some Widgets' text box. This issue affects Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41810**	https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/199
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). This vulnerability allowed Javascript code to be executed in the news section of the web console. This issue affects Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41811**	https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-ART-PAND-181223/200
Improper Neutralization of	23-Nov-2023	5.4	Improper Neutralization of Input During Web	https://pandorafms.com/en/security/commo	A-ART-PAND-181223/201

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
Input During Web Page Generation ('Cross-site Scripting')			Page Generation ('Cross-site Scripting') vulnerability in Pandora FMS on all allows Cross-Site Scripting (XSS). This vulnerability allowed users with low privileges to introduce Javascript executables via a translation string that could affect the integrity of some configuration files. This issue affects Pandora FMS: from 700 through 773. **CVE ID : CVE-2023-41791**	n-vulnerabilities-and-exposures/	
Vendor: asdqwedev					
Product: ajax_domain_checker					
Affected Version(s): * Up to (including) 1.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Asdqwe Dev Ajax Domain Checker plugin <= 1.3.0 versions. **CVE ID : CVE-2023-47810**	N/A	A-ASD-AJAX-181223/202
Vendor: Atlassian					
Product: bamboo					
Affected Version(s): From (including) 8.1.0 Up to (excluding) 9.2.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Nov-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability was introduced in versions 8.1.0, 8.2.0, 9.0.0, 9.1.0, 9.2.0, and 9.3.0 of Bamboo Data Center and Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Bamboo Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Bamboo Data Center and Server	https://confluence.atlassian.com/pages/viewpage.action?pageId=1318881573, https://jira.atlassian.com/browse/BAM-25168	A-ATL-BAMB-181223/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	9.2: Upgrade to a release greater than or equal to 9.2.7. JDK 1.8u121+ should be used in case Java 8 used to run Bamboo Data Center and Server. See Bamboo 9.2 Upgrade notes (https://confluence.atlassian.com/bambooreleases/bamboo-9-2-upgrade-notes-1207179212.html) Bamboo Data Center and Server 9.3: Upgrade to a release greater than or equal to 9.3.4 See the release notes ([https://confluence.atlassian.com/bambooreleases/bamboo-release-notes-1189793869.html]). You can download the latest version of Bamboo Data Center and Server from the download center ([https://www.atlassian.com/software/bamboo/download-archives]).		

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
			This vulnerability was discovered by a private user and reported via our Bug Bounty program **CVE ID : CVE-2023-22516**		
Affected Version(s): From (including) 9.3.0 Up to (excluding) 9.3.4					
N/A	21-Nov-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability was introduced in versions 8.1.0, 8.2.0, 9.0.0, 9.1.0, 9.2.0, and 9.3.0 of Bamboo Data Center and Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Bamboo Data	https://confluence.atlassian.com/pages/viewpage.action?pageId=1318881573, https://jira.atlassian.com/browse/BAM-25168	A-ATL-BAMB-181223/204

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
			Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Bamboo Data Center and Server 9.2: Upgrade to a release greater than or equal to 9.2.7. JDK 1.8u121+ should be used in case Java 8 used to run Bamboo Data Center and Server. See Bamboo 9.2 Upgrade notes (https://confluence.atlassian.com/bambooreleases/bamboo-9-2-upgrade-notes-1207179212.html) Bamboo Data Center and Server 9.3: Upgrade to a release greater than or equal to 9.3.4 See the release notes ([https://confluence.atlassian.com/bambooreleases/bamboo-release-notes-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1189793869.html]). You can download the latest version of Bamboo Data Center and Server from the download center ([https://www.atlassian.com/software/bamboo/download-archives]). This vulnerability was discovered by a private user and reported via our Bug Bounty program **CVE ID : CVE-2023-22516**		
Product: crowd					
Affected Version(s): 5.2.0					
N/A	21-Nov-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 3.4.6 of Crowd Data Center and Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.0, allows an authenticated attacker to execute arbitrary code which has high impact to	https://confluence.atlassian.com/pages/viewpage.action?pageId=1318881573, https://jira.atlassian.com/browse/CWD-6139	A-ATL-CROW-181223/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Crowd Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Crowd Data Center and Server 3.4: Upgrade to a release greater than or equal to 5.1.6 Crowd Data Center and Server 5.2: Upgrade to a release greater than or equal to 5.2.1 See the release notes ([https://confluence.atlassian.com/crowd/crowd-release-notes-199094.html]). You can download the latest version of Crowd Data Center		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Server from the download center ([https://www.atlassian.com/software/crowd/download-archive]). This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program **CVE ID : CVE-2023-22521**		
Affected Version(s): From (including) 3.4.0 Up to (excluding) 5.1.6					
N/A	21-Nov-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 3.4.6 of Crowd Data Center and Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.0, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction.	https://confluence.atlassian.com/pages/viewpage.action?pageId=1318881573, https://jira.atlassian.com/browse/CWD-6139	A-ATL-CROW-181223/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Atlassian recommends that Crowd Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Crowd Data Center and Server 3.4: Upgrade to a release greater than or equal to 5.1.6 Crowd Data Center and Server 5.2: Upgrade to a release greater than or equal to 5.2.1 See the release notes ([https://confluence.atlassian.com/crowd/crowd-release-notes-199094.html]). You can download the latest version of Crowd Data Center and Server from the download center ([https://www.atlassian.com/software/crowd/download-archive]).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program **CVE ID : CVE-2023-22521**		
Vendor: Autodesk					
Product: autocad					
Affected Version(s): * Up to (excluding) 2024.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/207
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/209
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/211
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-41140		
Affected Version(s): From (including) 2023.0.0 Up to (excluding) 2023.1.4					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/213
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/214

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-2023-29074		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/215
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29076		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/217
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/218
Affected Version(s): From (including) 2024.0.0 Up to (excluding) 2024.1.1					

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
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/219
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/221
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/222
Improper Restriction of	23-Nov-2023	7.8	A maliciously crafted STP file when parsed	https://www.autodesk.com/trust/security-	A-AUT-AUTO-181223/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	advisories/adsk-sa-2023-0018	
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/224
Product: autocad_advance_steel					
Affected Version(s): From (including) 2024.0.0 Up to (excluding) 2024.1.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-181223/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	k-sa-2023-0018	
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/226
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/228
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**		
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/230
Affected Version(s): * Up to (excluding) 2023.1.4					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the current process. **CVE ID : CVE-2023-29073**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/232
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2023-29075**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/234
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/236
Product: autocad_architecture					
Affected Version(s): From (including) 2024.0.0 Up to (excluding) 2024.1.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29073		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/238
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/240
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/241
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**		
Affected Version(s): * Up to (excluding) 2023.1.4					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/243
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/245
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/246

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
			vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/247
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2023-41140**		
Product: autocad_civil_3d					
Affected Version(s): From (including) 2024.0.0 Up to (excluding) 2024.1.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/249
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the current process. **CVE ID : CVE-2023-29074**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/251
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29076		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/253
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/254
Affected Version(s): * Up to (excluding) 2023.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/255
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/257
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/258
Improper Restriction of	23-Nov-2023	7.8	A maliciously crafted STP file when parsed	https://www.autodesk.com/trust/security-	A-AUT-AUTO-181223/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	advisories/adsk-sa-2023-0018	
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/260
Product: autocad_electrical					
Affected Version(s): From (including) 2024.0.0 Up to (excluding) 2024.1.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-AUTO-181223/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	k-sa-2023-0018	
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/262
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/264
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**		
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/266
Affected Version(s): * Up to (excluding) 2023.1.4					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the current process. **CVE ID : CVE-2023-29073**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/268
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2023-29075**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/270
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/272
Product: autocad_lt					
Affected Version(s): * Up to (excluding) 2024.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29073		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/274
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/276
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/277
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**		
Affected Version(s): From (including) 2024.0.0 Up to (excluding) 2024.1.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/279
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/281
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/283
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2023-41140**		
Affected Version(s): * Up to (excluding) 2023.1.4					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/285
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2023-29074**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/287
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29076		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/289
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/290
Product: autocad_map_3d					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2024.0.0 Up to (excluding) 2024.1.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/291
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/293
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/294
Improper Restriction of	23-Nov-2023	7.8	A maliciously crafted STP file when parsed	https://www.autodesk.com/trust/security-	A-AUT-AUTO-181223/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	advisories/adsk-sa-2023-0018	
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/296
Affected Version(s): * Up to (excluding) 2023.1.4					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/298
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/300
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the current process. **CVE ID : CVE-2023-41139**		
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/302
Product: autocad_mechanical					
Affected Version(s): From (including) 2024.0.0 Up to (excluding) 2024.1.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the current process. **CVE ID : CVE-2023-29073**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/304
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2023-29075**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/306
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/308
Affected Version(s): * Up to (excluding) 2023.1.4					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/310
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/311
Improper Restriction	23-Nov-2023	9.8	A maliciously crafted MODEL,	https://www.autodesk.com/tr	A-AUT-AUTO-181223/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	ust/security-advisories/adsk-sa-2023-0018	
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/313
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**		
Product: autocad_mep					
Affected Version(s): From (including) 2024.0.0 Up to (excluding) 2024.1.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/315
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/317
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/319
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2023-41140**		
Affected Version(s): * Up to (excluding) 2023.1.4					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/321
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the current process. **CVE ID : CVE-2023-29074**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/323
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29076		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/325
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/326
Product: autocad_plant_3d					

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 Version(s): From (including) 2024.0.0 Up to (excluding) 2024.1.1					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/327
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/329
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/330
Improper Restriction of	23-Nov-2023	7.8	A maliciously crafted STP file when parsed	https://www.autodesk.com/trust/security-	A-AUT-AUTO-181223/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-41139**	advisories/adsk-sa-2023-0018	
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/332
Affected Version(s): * Up to (excluding) 2023.1.4					
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted MODEL file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29073**		
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29074**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/334
Out-of-bounds Write	23-Nov-2023	9.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause an Out-Of-Bounds Write. A malicious actor can	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-29075**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	9.8	A maliciously crafted MODEL, SLDASM, SAT or CATPART file when parsed through Autodesk AutoCAD 2024 and 2023 could cause memory corruption vulnerability. This vulnerability, along with other vulnerabilities, could lead to code execution in the current process. **CVE ID : CVE-2023-29076**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/336
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Nov-2023	7.8	A maliciously crafted STP file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to dereference an untrusted pointer. This vulnerability, along with other vulnerabilities, could lead to code	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the current process. **CVE ID : CVE-2023-41139**		
Out-of-bounds Write	23-Nov-2023	7.8	A maliciously crafted PRT file when parsed through Autodesk AutoCAD 2024 and 2023 can be used to cause a Heap-Based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-41140**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018	A-AUT-AUTO-181223/338
Product: customer_portal					
Affected Version(s): -					
N/A	22-Nov-2023	5.3	Autodesk users who no longer have an active license for an account can still access cases for that account. **CVE ID : CVE-2023-41145**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0020	A-AUT-CUST-181223/339
N/A	22-Nov-2023	4.3	Autodesk Customer Support Portal allows cases created by users	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-CUST-181223/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			under an account to see cases created by other users on the same account. **CVE ID : CVE-2023-41146**	k-sa-2023-0020	
Product: desktop_connector					
Affected Version(s): * Up to (including) 16.2.1.2016					
Uncontrolled Search Path Element	22-Nov-2023	7.8	A maliciously crafted DLL file can be forced to install onto a non-default location, and attacker can overwrite parts of the product with malicious DLLs. These files may then have elevated privileges leading to a Privilege Escalation vulnerability. **CVE ID : CVE-2023-29069**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0013	A-AUT-DESK-181223/341
Vendor: averta					
Product: master_slider					
Affected Version(s): * Up to (including) 3.6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Averta Master Slider Pro plugin <= 3.6.5 versions. **CVE ID : CVE-2023-47508**	N/A	A-AVE-MAST-181223/342
Vendor: aweber					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: aweber					
Affected Version(s): * Up to (excluding) 7.3.10					
Cross-Site Request Forgery (CSRF)	17-Nov-2023	8.8	Missing Authorization, Cross-Site Request Forgery (CSRF) vulnerability in AWeber AWeber – Free Sign Up Form and Landing Page Builder Plugin for Lead Generation and Email Newsletter Growth allows Accessing Functionality Not Properly Constrained by ACLs, Cross-Site Request Forgery.This issue affects AWeber – Free Sign Up Form and Landing Page Builder Plugin for Lead Generation and Email Newsletter Growth: from n/a through 7.3.9. **CVE ID : CVE-2023-47757**	N/A	A-AWE-AWEB-181223/343
Vendor: ays-pro					
Product: popup_box					
Affected Version(s): * Up to (excluding) 3.7.9					
Improper Neutralization of Input	20-Nov-2023	4.8	The Popup box WordPress plugin before 3.7.9 does not sanitise and	N/A	A-AYS-POPU-181223/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed. **CVE ID : CVE-2023-5343**		
Vendor: bamboo_mcr					
Product: bamboo_columns					
Affected Version(s): * Up to (including) 1.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bamboo Mcr Bamboo Columns plugin <= 1.6.1 versions. **CVE ID : CVE-2023-47812**	N/A	A-BAM-BAMB-181223/345
Vendor: bandoche					
Product: pypinksign					
Affected Version(s): 0.5.1					
Use of Insufficiently Random Values	16-Nov-2023	7.5	PyPinkSign v0.5.1 uses a non-random or static IV for Cipher Block Chaining (CBC) mode in AES encryption. This vulnerability can lead to the disclosure of	N/A	A-BAN-PYPI-181223/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information and communications. **CVE ID : CVE-2023-48056**		
Vendor: bdaia					
Product: woohoo_newspaper_magazine_theme					
Affected Version(s): * Up to (including) 1.4.3					
Cross-Site Request Forgery (CSRF)	20-Nov-2023	8.8	The WooHoo Newspaper Magazine theme 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-2023-4824**	N/A	A-BDA-WOOH-181223/347
Vendor: bmicalculator					
Product: bmi_calculator					
Affected Version(s): * Up to (including) 1.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Waterloo Plugins BMI Calculator Plugin plugin <= 1.0.3 versions. **CVE ID : CVE-2023-47814**	N/A	A-BMI-BMI_-181223/348
Vendor: bookstackapp					
Product: book_stack					

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 Version(s): 23.10.2					
Server-Side Request Forgery (SSRF)	20-Nov-2023	6.5	Book Stack version 23.10.2 allows filtering local files on the server. This is possible because the application is vulnerable to SSRF. **CVE ID : CVE-2023-6199**	https://www.bookstackapp.com/blog/bookstack-release-v23-10-3/	A-BOO-BOOK-181223/349
Vendor: booster					
Product: booster_for_woocommerce					
Affected Version(s): * Up to (including) 7.1.1					
N/A	23-Nov-2023	6.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Pluggabl LLC Booster for WooCommerce plugin <= 7.1.1 versions. **CVE ID : CVE-2023-40002**	N/A	A-BOO-BOOS-181223/350
Vendor: botanikyazilim					
Product: pharmacy_automation					
Affected Version(s): * Up to (excluding) 2.1.133.0					
N/A	22-Nov-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Botanik Software Pharmacy Automation allows Retrieve Embedded Sensitive Data.This issue affects	N/A	A-BOT-PHAR-181223/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Pharmacy Automation: before 2.1.133.0. **CVE ID : CVE-2023-5983**		
Vendor: Bouncycastle					
Product: bouncy_castle_for_java					
Affected Version(s): * Up to (excluding) 1.73					
Uncontrolled Resource Consumption	23-Nov-2023	5.5	Bouncy Castle for Java before 1.73 contains a potential Denial of Service (DoS) issue within the Bouncy Castle org.bouncycastle.openssl.PEMParser class. This class parses OpenSSL PEM encoded streams containing X.509 certificates, PKCS8 encoded keys, and PKCS7 objects. Parsing a file that has crafted ASN.1 data through the PEMParser causes an OutOfMemoryError, which can enable a denial of service attack. **CVE ID : CVE-2023-33202**	N/A	A-BOU-BOUN-181223/352
Vendor: Busybox					
Product: busybox					
Affected Version(s): 1.36.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	27-Nov-2023	5.5	A use-after-free vulnerability was discovered in xasprintf function in xfuncs_printf.c:344 in BusyBox v.1.36.1. **CVE ID : CVE-2023-42363**	https://bugs.busybox.net/show_bug.cgi?id=15865	A-BUS-BUSY-181223/353
Use After Free	27-Nov-2023	5.5	A use-after-free vulnerability in BusyBox v.1.36.1 allows attackers to cause a denial of service via a crafted awk pattern in the awk.c evaluate function. **CVE ID : CVE-2023-42364**	https://bugs.busybox.net/show_bug.cgi?id=15868	A-BUS-BUSY-181223/354
Use After Free	27-Nov-2023	5.5	A use-after-free vulnerability was discovered in BusyBox v.1.36.1 via a crafted awk pattern in the awk.c copyvar function. **CVE ID : CVE-2023-42365**	https://bugs.busybox.net/show_bug.cgi?id=15871	A-BUS-BUSY-181223/355
Out-of-bounds Write	27-Nov-2023	5.5	A heap-buffer-overflow was discovered in BusyBox v.1.36.1 in the next_token function at awk.c:1159. **CVE ID : CVE-2023-42366**	https://bugs.busybox.net/show_bug.cgi?id=15874	A-BUS-BUSY-181223/356
Vendor: bytecodealliance					
Product: webassembly_micro_runtime					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.2.3					
Out-of-bounds Write	22-Nov-2023	7.5	An heap overflow vulnerability was discovered in Bytecode alliance wasm-micro-runtime v.1.2.3 allows a remote attacker to cause a denial of service via the wasm_loader_prepare_bytecode function in core/iwasm/interpreter/wasm_loader.c. **CVE ID : CVE-2023-48105**	https://github.com/bytecodealliance/wasm-micro-runtime/issues/2726, https://github.com/bytecodealliance/wasm-micro-runtime/pull/2734/commits/4785d91b16dd49c09a96835de2d9c7b077543fa4	A-BYT-WEBA-181223/357
Vendor: Capnproto					
Product: capnproto					
Affected Version(s): 1.0.0					
Out-of-bounds Write	21-Nov-2023	9.8	Cap'n Proto is a data interchange format and capability-based RPC system. In versions 1.0 and 1.0.1, when using the KJ HTTP library with WebSocket compression enabled, a buffer underrun can be caused by a remote peer. The underrun always writes a constant value that is not attacker-controlled, likely resulting in a crash, enabling a remote	https://github.com/capnproto/capnproto/security/advisories/GHSA-r89h-f468-62w3, https://github.com/capnproto/capnproto/commit/75c5c1499aa6e7690b741204ff9af91cce526c59, https://github.com/capnproto/capnproto/commit/e7f22da9c01286a2b0e1e5fbdf3ec9ab3aa128ff	A-CAP-CAPN-181223/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	denial-of-service attack. Most Cap'n Proto and KJ users are unlikely to have this functionality enabled and so unlikely to be affected. Maintainers suspect only the Cloudflare Workers Runtime is affected. If KJ HTTP is used with WebSocket compression enabled, a malicious peer may be able to cause a buffer underrun on a heap-allocated buffer. KJ HTTP is an optional library bundled with Cap'n Proto, but is not directly used by Cap'n Proto. WebSocket compression is disabled by default. It must be enabled via a setting passed to the KJ HTTP library via `HttpClientSettings` or `HttpServerSettings`. The bytes written out-of-bounds are always a specific constant 4-byte string `{ 0x00, 0x00, 0xFF, 0xFF }`.		

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
			Because this string is not controlled by the attacker, maintainers believe it is unlikely that remote code execution is possible. However, it cannot be ruled out. This functionality first appeared in Cap'n Proto 1.0. Previous versions are not affected. This issue is fixed in Cap'n Proto 1.0.1.1. **CVE ID : CVE-2023-48230**		
Affected Version(s): 1.0.1					
Out-of-bounds Write	21-Nov-2023	9.8	Cap'n Proto is a data interchange format and capability-based RPC system. In versions 1.0 and 1.0.1, when using the KJ HTTP library with WebSocket compression enabled, a buffer underrun can be caused by a remote peer. The underrun always writes a constant value that is not attacker-controlled, likely resulting in a crash, enabling a remote	https://github.com/capnproto/capnproto/security/advisories/GHSA-r89h-f468-62w3, https://github.com/capnproto/capnproto/commit/75c5c1499aa6e7690b741204ff9af91cce526c59, https://github.com/capnproto/capnproto/commit/e7f22da9c01286a2b0e1e5fbdf3ec9ab3aa128ff	A-CAP-CAPN-181223/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial-of-service attack. Most Cap'n Proto and KJ users are unlikely to have this functionality enabled and so unlikely to be affected. Maintainers suspect only the Cloudflare Workers Runtime is affected. If KJ HTTP is used with WebSocket compression enabled, a malicious peer may be able to cause a buffer underrun on a heap-allocated buffer. KJ HTTP is an optional library bundled with Cap'n Proto, but is not directly used by Cap'n Proto. WebSocket compression is disabled by default. It must be enabled via a setting passed to the KJ HTTP library via `HttpClientSettings` or `HttpServerSettings`. The bytes written out-of-bounds are always a specific constant 4-byte string `{ 0x00, 0x00, 0xFF, 0xFF }`.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Because this string is not controlled by the attacker, maintainers believe it is unlikely that remote code execution is possible. However, it cannot be ruled out. This functionality first appeared in Cap'n Proto 1.0. Previous versions are not affected. This issue is fixed in Cap'n Proto 1.0.1.1. **CVE ID : CVE-2023-48230**		
Vendor: carglglz					
Product: upydev					
Affected Version(s): 0.4.3					
Inadequate Encryption Strength	20-Nov-2023	7.5	An issue in /upydev/keygen.py in upydev v0.4.3 allows attackers to decrypt sensitive information via weak encryption padding. **CVE ID : CVE-2023-48051**	N/A	A-CAR-UPYD-181223/360
Vendor: Chamilo					
Product: chamilo_lms					
Affected Version(s): * Up to (including) 1.11.24					
Improper Neutralization of	28-Nov-2023	8.8	Command injection in `main/lp/openoffic	https://support.chamilo.org/projects/chamil	A-CHA-CHAM-181223/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			e_presentation.class.php` in Chamilo LMS <= v1.11.24 allows users permitted to upload Learning Paths to obtain remote code execution via improper neutralisation of special characters. **CVE ID : CVE-2023-4221**	o-18/wiki/security_issues#Issue-128-2023-09-04-Critical-impact-Moderate-risk-Authenticated-users-may-gain-unauthenticated-RCE-CVE-2023-4221CVE-2023-4222	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Nov-2023	8.8	Command injection in `main/lp/openoffice_text_document.class.php` in Chamilo LMS <= v1.11.24 allows users permitted to upload Learning Paths to obtain remote code execution via improper neutralisation of special characters. **CVE ID : CVE-2023-4222**	https://support.chamilo.org/projects/chamilo-18/wiki/security_issues#Issue-128-2023-09-04-Critical-impact-Moderate-risk-Authenticated-users-may-gain-unauthenticated-RCE-CVE-2023-4221CVE-2023-4222	A-CHA-CHAM-181223/362
Unrestricted Upload of File with Dangerous Type	28-Nov-2023	8.8	Unrestricted file upload in `/main/inc/ajax/document.ajax.php` in Chamilo LMS <= v1.11.24 allows authenticated attackers with learner role to obtain remote code	https://support.chamilo.org/projects/chamilo-18/wiki/security_issues#Issue-129-2023-09-04-Critical-impact-Moderate-risk-	A-CHA-CHAM-181223/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution via uploading of PHP files. **CVE ID : CVE-2023-4223**	Authenticated-users-may-gain-unauthenticated-RCE-CVE-2023-4223CVE-2023-4224CVE-2023-4225CVE-2023-4226	
Unrestricted Upload of File with Dangerous Type	28-Nov-2023	8.8	Unrestricted file upload in `/main/inc/ajax/dropbox.ajax.php` in Chamilo LMS <= v1.11.24 allows authenticated attackers with learner role to obtain remote code execution via uploading of PHP files. **CVE ID : CVE-2023-4224**	https://support.chamilo.org/projects/chamilo-18/wiki/security_issues#Issue-129-2023-09-04-Critical-impact-Moderate-risk-Authenticated-users-may-gain-unauthenticated-RCE-CVE-2023-4223CVE-2023-4224CVE-2023-4225CVE-2023-4226	A-CHA-CHAM-181223/364
Unrestricted Upload of File with Dangerous Type	28-Nov-2023	8.8	Unrestricted file upload in `/main/inc/ajax/exercise.ajax.php` in Chamilo LMS <= v1.11.24 allows authenticated attackers with learner role to	https://support.chamilo.org/projects/chamilo-18/wiki/security_issues#Issue-129-2023-09-04-Critical-impact-	A-CHA-CHAM-181223/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain remote code execution via uploading of PHP files. **CVE ID : CVE-2023-4225**	Moderate-risk-Authenticated-users-may-gain-unauthenticated-RCE-CVE-2023-4223CVE-2023-4224CVE-2023-4225CVE-2023-4226	
Unrestricted Upload of File with Dangerous Type	28-Nov-2023	8.8	Unrestricted file upload in `/main/inc/ajax/work.ajax.php` in Chamilo LMS <= v1.11.24 allows authenticated attackers with learner role to obtain remote code execution via uploading of PHP files. **CVE ID : CVE-2023-4226**	https://support.chamilo.org/projects/chamilo-18/wiki/security_issues#Issue-129-2023-09-04-Critical-impact-Moderate-risk-Authenticated-users-may-gain-unauthenticated-RCE-CVE-2023-4223CVE-2023-4224CVE-2023-4225CVE-2023-4226	A-CHA-CHAM-181223/366
Vendor: christinauechi					
Product: add_widgets_to_page					
Affected Version(s): * Up to (including) 1.3.2					
Improper Neutralization of Input	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation	N/A	A-CHR-ADD_-181223/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			('Cross-site Scripting') vulnerability in Christina Uechi Add Widgets to Page plugin <= 1.3.2 versions. **CVE ID : CVE-2023-47808**		
Vendor: chronopost					
Product: chronopost					
Affected Version(s): * Up to (including) 6.2.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Nov-2023	9.8	In the module "Chronopost Official" (chronopost) for PrestaShop, a guest can perform SQL injection. The script PHP `cancelSkybill.php` own a sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection. **CVE ID : CVE-2023-45377**	https://security.friendsofpresta.org/modules/2023/11/21/chronopost.html	A-CHR-CHRO-181223/368
Vendor: Ciphercoin					
Product: easy_hide_login					
Affected Version(s): * Up to (including) 1.0.8					
N/A	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Arshid Easy Hide Login.This issue affects Easy Hide Login: from n/a through 1.0.8.	N/A	A-CIP-EASY-181223/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31075		
Vendor: Cisco					
Product: anyconnect_secure_mobility_client					
Affected Version(s): 4.9.00086					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-ANYC-181223/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.9.01095					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-ANYC-181223/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.9.02028					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-ANYC-181223/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.9.03047					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-ANYC-181223/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.9.03049					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-ANYC-181223/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.9.04043					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-ANYC-181223/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.9.04053					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-ANYC-181223/376

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
			accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.9.05042					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-ANYC-181223/377

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
			Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.9.06037					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-ANYC-181223/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Product: appdynamics					
Affected Version(s): 21.2.7					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco	https://sec.cloudapps.cisco.com/security/cen	A-CIS-APPD-181223/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**	ter/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	
Affected Version(s): 21.2.8					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-	A-CIS-APPD-181223/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**	authpriv-gEBwTvu5	
Affected Version(s): 21.4.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/381

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
			This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 21.4.10					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 21.4.11					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 21.4.2					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 21.4.3					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 21.4.4					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 21.4.5					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20274		
Affected Version(s): 21.4.6					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/388
Affected Version(s): 21.4.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/389
Affected Version(s): 21.4.8					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP	https://sec.cloudapps.cisco.com/security/center/content/Cis	A-CIS-APPD-181223/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**	coSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	
Affected Version(s): 21.4.9					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-	A-CIS-APPD-181223/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**	authpriv-gBEwTvu5	
Affected Version(s): 21.5.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gBEwTvu5	A-CIS-APPD-181223/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 21.6.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 21.7.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 22.1.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 22.1.1					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 22.10.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 22.11.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20274		
Affected Version(s): 22.12.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/399
Affected Version(s): 22.12.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/400
Affected Version(s): 22.3.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP	https://sec.cloudapps.cisco.com/security/center/content/Cis	A-CIS-APPD-181223/401

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
			Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**	coSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	
Affected Version(s): 22.8.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-	A-CIS-APPD-181223/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**	authpriv-gEBwTvu5	
Affected Version(s): 23.2.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Affected Version(s): 23.4.0					
N/A	21-Nov-2023	7.8	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-php-authpriv-gEBwTvu5	A-CIS-APPD-181223/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device. **CVE ID : CVE-2023-20274**		
Product: identity_services_engine					
Affected Version(s): 3.0.0					
N/A	21-Nov-2023	8.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine could allow an authenticated, remote attacker to upload malicious files to the web root of the application. This vulnerability is due to insufficient file input validation. An attacker could exploit this vulnerability by uploading a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-j-KxpNynR	A-CIS-IDEN-181223/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious file to the web interface. A successful exploit could allow the attacker to replace files and gain access to sensitive server-side information. **CVE ID : CVE-2023-20272**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	4.8	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to conduct an XSS attack against a user of the web-based management interface of an affected device. **CVE ID : CVE-2023-20208**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-j-KxpNynR	A-CIS-IDEN-181223/406
Affected Version(s): 3.1					
N/A	21-Nov-2023	8.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine could allow an authenticated, remote attacker to upload malicious files to the web root of the application. This vulnerability is due to insufficient file input validation. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-j-KxpNynR	A-CIS-IDEN-181223/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by uploading a malicious file to the web interface. A successful exploit could allow the attacker to replace files and gain access to sensitive server-side information. **CVE ID : CVE-2023-20272**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	4.8	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to conduct an XSS attack against a user of the web-based management interface of an affected device. **CVE ID : CVE-2023-20208**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-j-KxpNynR	A-CIS-IDEN-181223/408
Affected Version(s): 3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	4.8	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to conduct an XSS attack against a user of the web-based management	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-j-KxpNynR	A-CIS-IDEN-181223/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of an affected device. **CVE ID : CVE-2023-20208**		
Product: secure_client					
Affected Version(s): 4.10.00093					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/410

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
			crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.01075					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/411

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
			Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.02086					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.03104					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.04065					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvi	A-CIS-SECU-181223/414

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
			Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system.	sory/cisco-sa-accsc-dos-9SLzkZ8	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20241		
Affected Version(s): 4.10.04071					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.05085					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.05095					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.05111					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/418

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.06079					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/419

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
			denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.06090					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.07061					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/421

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
			the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.07062					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/422

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
			accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 4.10.07073					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/423

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 5.0.00238					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 5.0.00529					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvi	A-CIS-SECU-181223/425

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
			Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system.	sory/cisco-sa-accsc-dos-9SLzkZ8	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20241		
Affected Version(s): 5.0.00556					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 5.0.01242					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 5.0.02075					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 5.0.03072					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Affected Version(s): 5.0.03076					
Out-of-bounds Read	22-Nov-2023	5.5	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-dos-9SLzkZ8	A-CIS-SECU-181223/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system. **CVE ID : CVE-2023-20241**		
Vendor: cksource					
Product: ckeditor					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 4.15.1					
N/A	16-Nov-2023	6.1	A Cross-Site scripting vulnerability has been found in CKSource CKEditor affecting versions 4.15.1 and earlier. An attacker could send malicious javascript code through the /ckeditor/samples/old/ajax.html file and retrieve an authorized user's information. **CVE ID : CVE-2023-4771**	N/A	A-CKS-CKED-181223/431
Vendor: clastix					
Product: capsule-proxy					
Affected Version(s): * Up to (including) 0.4.5					
Improper Authentication	24-Nov-2023	9.8	capsule-proxy is a reverse proxy for the capsule operator project. Affected versions are subject to a privilege escalation vulnerability which is based on a missing check if the user is authenticated based on the `TokenReview` result. All the clusters running with the `anonymous-auth` Kubernetes API Server setting	https://github.com/projectcapsule/capsule-proxy/security/advisories/GHSA-fpvw-6m5v-hqfp, https://github.com/projectcapsule/capsule-proxy/commit/472404f7006a4152e4eec76dee07324dd1e6e823	A-CLA-CAPS-181223/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disable (set to `false`) are affected since it would be possible to bypass the token review mechanism, interacting with the upper Kubernetes API Server. This privilege escalation cannot be exploited if you're relying only on client certificates (SSL/TLS). This vulnerability has been addressed in version 0.4.6. Users are advised to upgrade. **CVE ID : CVE-2023-48312**		
Vendor: Cminds					
Product: cm_on_demand_search_and_replace					
Affected Version(s): * Up to (including) 1.3.0					
N/A	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in CreativeMindsSolutions CM On Demand Search And Replace plugin <= 1.3.0 versions. **CVE ID : CVE-2023-28749**	N/A	A-CMI-CM_O-181223/433
Vendor: code-projects					
Product: simple_crud_functionality					
Affected Version(s): 1.0					
Improper Neutralization of	17-Nov-2023	9.8	SQL Injection vulnerability in add.php in Simple	N/A	A-COD-SIMP-181223/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			CRUD Functionality v1.0 allows attackers to run arbitrary SQL commands via the 'title' parameter. **CVE ID : CVE-2023-48078**		
Vendor: codebard					
Product: codebard\'s_patron_button_and_widgets_for_patreon					
Affected Version(s): * Up to (excluding) 2.2.0					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in CodeBard CodeBard's Patron Button and Widgets for Patreon plugin <= 2.1.9 versions. **CVE ID : CVE-2023-47765**	N/A	A-COD-CODE-181223/435
Vendor: codeboxr					
Product: cbx_currency_converter					
Affected Version(s): * Up to (including) 3.0.3					
N/A	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in codeboxr CBX Currency Converter plugin <= 3.0.3 versions. **CVE ID : CVE-2023-28747**	N/A	A-COD-CBX_-181223/436
Vendor: codebxr					
Product: cbx_map_for_google_map_\&_openstreetmap					
Affected Version(s): * Up to (including) 1.1.11					
Improper Neutralization of	16-Nov-2023	5.4	Auth. (contributor+) Stored Cross-Site	N/A	A-COD-CBX_-181223/437

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
Input During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability in Codeboxr CBX Map for Google Map & OpenStreetMap plugin <= 1.1.11 versions. **CVE ID : CVE-2023-47240**		
Vendor: codedropz					
Product: drag_and_drop_multiple_file_upload_-_contact_form_7					
Affected Version(s): * Up to (including) 1.3.7.3					
Unrestricted Upload of File with Dangerous Type	22-Nov-2023	9.8	The Drag and Drop Multiple File Upload - Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads to insufficient file type validation in the 'dnd_upload_cf7_upload' function in versions up to, and including, 1.3.7.3. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. This can be exploited if a user authorized to edit form, which means editor privileges or above, has added a 'multiple file	https://www.wordfence.com/threat-intel/vulnerabilities/id/1b3be300-5b7f-4844-8637-1bb8c939ed4c?source=cve	A-COD-DRAG-181223/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload' form field with '*' acceptable file types. **CVE ID : CVE-2023-5822**		
Vendor: Codeigniter					
Product: shield					
Affected Version(s): 1.0.0					
Cleartext Storage of Sensitive Information	24-Nov-2023	6.5	CodeIgniter Shield is an authentication and authorization provider for CodeIgniter 4. The `secretKey` value is an important key for HMAC SHA256 authentication and in affected versions was stored in the database in cleartext form. If a malicious person somehow had access to the data in the database, they could use the key and secretKey for HMAC SHA256 authentication to send requests impersonating that corresponding user. This issue has been addressed in version 1.0.0-beta.8. Users are advised to upgrade. There are no known workarounds for this vulnerability.	https://github.com/codeigniter4/shield/security/advisories/GHSA-v427-c49j-8w6x, https://github.com/codeigniter4/shield/commit/f77c6ae20275ac1245330a2b9a523bf7e6f6202f	A-COD-SHIE-181223/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48707		
Insertion of Sensitive Information into Log File	24-Nov-2023	6.5	CodeIgniter Shield is an authentication and authorization provider for CodeIgniter 4. In affected versions successful login attempts are recorded with the raw tokens stored in the log table. If a malicious person somehow views the data in the log table they can obtain a raw token which can then be used to send a request with that user's authority. This issue has been addressed in version 1.0.0-beta.8. Users are advised to upgrade. Users unable to upgrade should disable logging for successful login attempts by the configuration files. **CVE ID : CVE-2023-48708**	https://github.com/codeigniter4/shield/security/advisories/GHSA-j72f-h752-mx4w, https://github.com/codeigniter4/shield/commit/7e84c3fb3411294f70890819bfe51781bb9dc8e4	A-COD-SHIE-181223/440
Vendor: codemshop					
Product: mshop_my_site					
Affected Version(s): * Up to (including) 1.1.6					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in CodeMShop ????	N/A	A-COD-MSHO-181223/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			????? – MSHOP MY SITE.This issue affects ???? ????? – MSHOP MY SITE: from n/a through 1.1.6. **CVE ID : CVE-2023-47243**		
Vendor: codez					
Product: quick_call_button					
Affected Version(s): * Up to (including) 1.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	4.8	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codez Quick Call Button plugin <= 1.2.9 versions. **CVE ID : CVE-2023-47829**	N/A	A-COD-QUIC-181223/442
Vendor: code_snippets					
Product: code_snippets					
Affected Version(s): * Up to (including) 3.5.0					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Code Snippets Pro Code Snippets.This issue affects Code Snippets: from n/a through 3.5.0.	N/A	A-COD-CODE-181223/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47666		
Vendor: Color					
Product: demoiccmax					
Affected Version(s): 2023-11-09					
Out-of-bounds Read	18-Nov-2023	6.5	In International Color Consortium DemoIccMAX 3e7948b, CIccCLUT::Interp2d in IccTagLut.cpp in libSampleICC.a has an out-of-bounds read. **CVE ID : CVE-2023-48736**	N/A	A-COL-DEMO-181223/444
Vendor: common-services					
Product: sonice_retour					
Affected Version(s): * Up to (including) 2.1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Nov-2023	7.5	In the module "SoNice Retour" (sonice_retour) up to version 2.1.0 from Common-Services for PrestaShop, a guest can download personal information without restriction by performing a path traversal attack. Due to a lack of permissions control and a lack of control in the path name construction, a guest can perform a path traversal to view all files on the	N/A	A-COM-SONI-181223/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information system. **CVE ID : CVE-2023-45382**		
Vendor: communitydeveloper					
Product: amazzing_filter					
Affected Version(s): * Up to (including) 3.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Nov-2023	6.1	Cross Site Scripting (XSS) in Search filters in Prestashop Amazzing filter version up to version 3.2.5, allows remote attackers to inject arbitrary JavaScript code. **CVE ID : CVE-2023-48042**	N/A	A-COM-AMAZ-181223/446
Vendor: computy					
Product: bonus_for_woo					
Affected Version(s): * Up to (excluding) 5.8.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	6.1	The Bonus for Woo WordPress plugin before 5.8.3 does not sanitise and escape some parameters before outputting them back in pages, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin. **CVE ID : CVE-2023-5140**	N/A	A-COM-BONU-181223/447
Vendor: concretecms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: concrete_cms					
Affected Version(s): * Up to (excluding) 8.5.13					
Incorrect Default Permissions	17-Nov-2023	9.8	Concrete CMS before 8.5.13 and 9.x before 9.2.2 allows unauthorized access because directories can be created with insecure permissions. File creation functions (such as the Mkdir() function) gives universal access (0777) to created folders by default. Excessive permissions can be granted when creating a directory with permissions greater than 0755 or when the permissions argument is not specified. **CVE ID : CVE-2023-48648**	https://www.concretecms.org/about/project-news/security/2023-11-09-security-blog-about-updated-cves-and-new-release	A-CON-CONC-181223/448
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-2023	5.4	Concrete CMS before 8.5.13 and 9.x before 9.2.2 allows stored XSS on the Admin page via an uploaded file name. **CVE ID : CVE-2023-48649**	https://www.concretecms.org/about/project-news/security/2023-11-09-security-blog-about-updated-cves-and-new-release, https://github.com/concretecms/concretecm	A-CON-CONC-181223/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				s/pull/11695, https://github.com/concretecms/concretecms/pull/11739	
Affected Version(s): From (including) 9.0 Up to (excluding) 9.2.2					
Incorrect Default Permissions	17-Nov-2023	9.8	Concrete CMS before 8.5.13 and 9.x before 9.2.2 allows unauthorized access because directories can be created with insecure permissions. File creation functions (such as the Mkdir() function) gives universal access (0777) to created folders by default. Excessive permissions can be granted when creating a directory with permissions greater than 0755 or when the permissions argument is not specified. **CVE ID : CVE-2023-48648**	https://www.concretecms.org/about/project-news/security/2023-11-09-security-blog-about-updated-cves-and-new-release	A-CON-CONC-181223/450
Improper Neutralization of Input During Web Page Generation	17-Nov-2023	5.4	Concrete CMS before 8.5.13 and 9.x before 9.2.2 allows stored XSS on the Admin page via an uploaded file name.	https://www.concretecms.org/about/project-news/security/2023-11-09-security-blog-about-updated-cves-and-new-	A-CON-CONC-181223/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-48649**	release, https://github.com/concretecms/concretecms/pull/11695, https://github.com/concretecms/concretecms/pull/11739	
Vendor: connekthq					
Product: instant_images					
Affected Version(s): * Up to (including) 5.1.0.2					
N/A	22-Nov-2023	8.8	Server-Side Request Forgery (SSRF) vulnerability in Darren Cooney Instant Images plugin <= 5.1.0.2 versions. **CVE ID : CVE-2023-27451**	N/A	A-CON-INST-181223/452
Vendor: corebos					
Product: corebos					
Affected Version(s): * Up to (including) 8.0					
Improper Neutralization of Formula Elements in a CSV File	17-Nov-2023	8	Corebos 8.0 and below is vulnerable to CSV Injection. An attacker with low privileges can inject a malicious command into a table. This vulnerability is exploited when an administrator visits the user management section, exports the data to a CSV file, and then opens it,	N/A	A-COR-CORE-181223/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to the execution of the malicious payload on the administrator's computer. **CVE ID : CVE-2023-48029**		
Vendor: crushftp					
Product: crushftp					
Affected Version(s): * Up to (excluding) 10.5.2					
Improper Control of Dynamically-Managed Code Resources	18-Nov-2023	9.8	CrushFTP prior to 10.5.1 is vulnerable to Improperly Controlled Modification of Dynamically-Determined Object Attributes. **CVE ID : CVE-2023-43177**	N/A	A-CRU-CRUS-181223/454
Vendor: cskaza					
Product: cszcms					
Affected Version(s): 1.3.0					
N/A	27-Nov-2023	7.2	A vulnerability was found in CSZCMS 1.3.0 and classified as critical. Affected by this issue is some unknown functionality of the file \views\templates of the component File Manager Page. The manipulation leads to permission issues. The attack may be launched remotely. The exploit has been	N/A	A-CSK-CSZC-181223/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The identifier of this vulnerability is VDB-246128. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-6302**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Nov-2023	4.8	A vulnerability was found in CSZCMS 1.3.0. It has been classified as problematic. This affects an unknown part of the file /admin/settings/ of the component Site Settings Page. The manipulation of the argument Additional Meta Tag with the input <svg><animate onbegin=alert(1) attributeName=x dur=1s> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-246129 was assigned to this vulnerability. NOTE: The vendor	N/A	A-CSK-CSZC-181223/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-6303**		
Vendor: Cubecart					
Product: cubecart					
Affected Version(s): * Up to (excluding) 6.5.3					
Cross-Site Request Forgery (CSRF)	17-Nov-2023	8.1	Cross-site request forgery (CSRF) vulnerability in CubeCart prior to 6.5.3 allows a remote unauthenticated attacker to delete data in the system. **CVE ID : CVE-2023-38130**	https://forums.cubecart.com/topic/58736-cubecart-653-released-security-update/, https://jvn.jp/en/jp/JVN22220399/	A-CUB-CUBE-181223/457
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Nov-2023	7.2	CubeCart prior to 6.5.3 allows a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-47675**	https://forums.cubecart.com/topic/58736-cubecart-653-released-security-update/, https://jvn.jp/en/jp/JVN22220399/	A-CUB-CUBE-181223/458
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Nov-2023	6.5	Directory traversal vulnerability in CubeCart prior to 6.5.3 allows a remote authenticated attacker with an administrative privilege to delete	https://forums.cubecart.com/topic/58736-cubecart-653-released-security-update/, https://jvn.jp/	A-CUB-CUBE-181223/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directories and files in the system. **CVE ID : CVE-2023-42428**	en/jp/JVN22220399/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Nov-2023	4.9	Directory traversal vulnerability in CubeCart prior to 6.5.3 allows a remote authenticated attacker with an administrative privilege to obtain files in the system. **CVE ID : CVE-2023-47283**	https://forums.cubecart.com/topic/58736-cubecart-653-released-security-update/, https://jvn.jp/en/jp/JVN22220399/	A-CUB-CUBE-181223/460
Vendor: dangngocbinh					
Product: easy_call_now_by_thikshare					
Affected Version(s): * Up to (including) 1.1.0					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Dang Ngoc Binh Easy Call Now by ThikShare plugin <= 1.1.0 versions. **CVE ID : CVE-2023-47819**	N/A	A-DAN-EASY-181223/461
Vendor: dassault					
Product: 3dswymer_3dexperience_2022					
Affected Version(s): fp.cfa.2337					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	Stored Cross-site Scripting (XSS) vulnerabilities affecting 3DSwym in 3DSwymer from Release 3DEXPERIENCE R2022x through Release	https://www.3ds.com/vulnerability/advisories	A-DAS-3DSW-181223/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3DEXPERIENCE R2023x allow an attacker to execute arbitrary script code. **CVE ID : CVE-2023-5598**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	A stored Cross-site Scripting (XSS) vulnerability affecting 3DDashboard in 3DSwymer from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2023x allows an attacker to execute arbitrary script code. **CVE ID : CVE-2023-5599**	https://www.3ds.com/vulnerability/advisories	A-DAS-3DSW-181223/463
Product: 3dswymer_3dexperience_2023					
Affected Version(s): fp.cfa.2333					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	Stored Cross-site Scripting (XSS) vulnerabilities affecting 3DSwym in 3DSwymer from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2023x allow an attacker to execute arbitrary script code.	https://www.3ds.com/vulnerability/advisories	A-DAS-3DSW-181223/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5598		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	A stored Cross-site Scripting (XSS) vulnerability affecting 3DDashboard in 3DSwymer from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2023x allows an attacker to execute arbitrary script code. **CVE ID : CVE-2023-5599**	https://www.3ds.com/vulnerability/advisories	A-DAS-3DSW-181223/465
Vendor: davidvongries					
Product: ultimate_dashboard					
Affected Version(s): * Up to (including) 3.7.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	4.8	The Ultimate Dashboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 3.7.7. due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2991103%40ultimate-dashboard%2Ftrunk&old=2958955%40ultimate-dashboard%2Ftrunk&sfp_email=&sfph_mail=#file5	A-DAV-ULTI-181223/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-4726**		
Vendor: dazzlersoft					
Product: team_members_showcase					
Affected Version(s): * Up to (including) 1.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Dazzlersoft Team Members Showcase plugin <= 1.3.4 versions. **CVE ID : CVE-2023-32957**	N/A	A-DAZ-TEAM-181223/467
Vendor: dece					
Product: geodi					
Affected Version(s): * Up to (excluding) 8.0.0.27396					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	0	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DECE Software Geodi allows Stored XSS.This issue affects Geodi: before 8.0.0.27396.	N/A	A-DEC-GEOD-181223/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6011		
Vendor: decesoftware					
Product: geodi					
Affected Version(s): * Up to (excluding) 8.0.0.27396					
N/A	22-Nov-2023	7.1	Improper Enforcement of Behavioral Workflow vulnerability in DECE Software Geodi allows Functionality Bypass.This issue affects Geodi: before 8.0.0.27396. **CVE ID : CVE-2023-5921**	N/A	A-DEC-GEOD-181223/469
Vendor: Dedecms					
Product: dedecms					
Affected Version(s): 5.7					
Cross-Site Request Forgery (CSRF)	16-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in DedeCMS v5.7 in 110 backend management interface via /catalog_add.php, allows attackers to create crafted web pages due to a lack of verification of the token value of the submitted form.	N/A	A-DED-DEDE-181223/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43275		
Vendor: Dell					
Product: command|configure					
Affected Version(s): * Up to (excluding) 4.11.0					
N/A	23-Nov-2023	7.8	Dell Command | Configure, versions prior to 4.11.0, contains an improper access control vulnerability. A local malicious user could potentially modify files inside installation folder during application upgrade, leading to privilege escalation. **CVE ID : CVE-2023-43086**	https://www.dell.com/support/kbdoc/en-us/000218424/dsa-2023-387-security-update-for-a-dell-command-configure-vulnerability	A-DEL-COMM-181223/471
N/A	23-Nov-2023	7.8	Dell Command | Configure versions prior to 4.11.0, contain an improper access control vulnerability. A local malicious standard user could potentially exploit this vulnerability while repairing/changing installation, leading	https://www.dell.com/support/kbdoc/en-us/000218628/dsa-2023-390-security-update-for-dell-command-configure-and-dell-command-monitor-vulnerabilities	A-DEL-COMM-181223/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to privilege escalation. **CVE ID : CVE-2023-44289**		
Product: command|monitor					
Affected Version(s): * Up to (excluding) 10.10.0					
N/A	23-Nov-2023	7.8	Dell Command | Monitor versions prior to 10.10.0, contain an improper access control vulnerability. A local malicious standard user could potentially exploit this vulnerability while repairing/changing installation, leading to privilege escalation. **CVE ID : CVE-2023-44290**	https://www.dell.com/support/kbdoc/en-us/000218628/dsa-2023-390-security-update-for-dell-command-configure-and-dell-command-monitor-vulnerabilities	A-DEL-COMM-181223/473
Product: e-lab_navigator					
Affected Version(s): 3.1.8					
Use of Hard-coded Credentials	16-Nov-2023	5.5	Dell ELab-Navigator, version 3.1.9 contains a hard-coded credential vulnerability. A local attacker could	https://www.dell.com/support/kbdoc/en-us/000219558/dsa-2023-419-security-update-for-mobility-e-lab-	A-DEL-E-LA-181223/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit this vulnerability, leading to unauthorized access to sensitive data. Successful exploitation may result in the compromise of confidential user information. **CVE ID : CVE-2023-44296**	navigator-vulnerabilities	
Affected Version(s): 3.1.9					
Use of Hard-coded Credentials	16-Nov-2023	5.5	Dell ELab-Navigator, version 3.1.9 contains a hard-coded credential vulnerability. A local attacker could potentially exploit this vulnerability, leading to unauthorized access to sensitive data. Successful exploitation may result in the compromise of confidential user information. **CVE ID : CVE-2023-44296**	https://www.dell.com/support/kbdoc/en-us/000219558/dsa-2023-419-security-update-for-mobility-e-lab-navigator-vulnerabilities	A-DEL-E-LA-181223/475
Product: encryption					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 11.8.1					
Improper Link Resolution Before File Access ('Link Following')	16-Nov-2023	7.3	Dell Encryption, Dell Endpoint Security Suite Enterprise, and Dell Security Management Server version prior to 11.8.1 contain an Insecure Operation on Windows Junction Vulnerability during installation. A local malicious user could potentially exploit this vulnerability to create an arbitrary folder inside a restricted directory, leading to Privilege Escalation **CVE ID : CVE-2023-39246**	https://www.dell.com/support/kbdoc/en-us/000217572/dsa-2023-271	A-DEL-ENCR-181223/476
Product: endpoint_security_suite_enterprise					
Affected Version(s): * Up to (excluding) 11.8.1					
Improper Link Resolution Before File Access ('Link Following')	16-Nov-2023	7.3	Dell Encryption, Dell Endpoint Security Suite Enterprise, and Dell Security Management Server version prior to 11.8.1 contain an Insecure	https://www.dell.com/support/kbdoc/en-us/000217572/dsa-2023-271	A-DEL-ENDP-181223/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Operation on Windows Junction Vulnerability during installation. A local malicious user could potentially exploit this vulnerability to create an arbitrary folder inside a restricted directory, leading to Privilege Escalation **CVE ID : CVE-2023-39246**		
Product: powerprotect_agent_for_file_system					
Affected Version(s): * Up to (including) 19.14					
Incorrect Default Permissions	22-Nov-2023	3.3	PowerProtect Agent for File System Version 19.14 and prior, contains an incorrect default permissions vulnerability in ddfscon component. A low Privileged local attacker could potentially exploit this vulnerability, leading to overwriting of log files.	https://www.dell.com/support/kbdoc/en-us/000219782/dsa-2023-427-security-update-for-dell-powerprotect-agent-for-file-system-vulnerabilities	A-DEL-POWE-181223/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43081		
Product: repository_manager					
Affected Version(s): * Up to (excluding) 3.4.4					
Improper Privilege Management	16-Nov-2023	7.8	Dell Repository Manager, 3.4.3 and prior, contains an Improper Access Control vulnerability in its installation module. A local low-privileged attacker could potentially exploit this vulnerability, leading to gaining escalated privileges. **CVE ID : CVE-2023-44292**	https://www.dell.com/support/kbdoc/en-us/000219303/dsa-2023-415-security-update-for-dell-repository-manager-vulnerability	A-DEL-REPO-181223/479
Affected Version(s): * Up to (including) 3.4.3					
Improper Privilege Management	16-Nov-2023	7.8	Dell Repository Manager, 3.4.3 and prior, contains an Improper Access Control vulnerability in its installation module. A local low-privileged attacker could potentially exploit this vulnerability, leading to gaining	https://www.dell.com/support/kbdoc/en-us/000219303/dsa-2023-415-security-update-for-dell-repository-manager-vulnerability	A-DEL-REPO-181223/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalated privileges. **CVE ID : CVE-2023-44282**		
Product: security_management_server					
Affected Version(s): * Up to (excluding) 11.8.1					
Improper Link Resolution Before File Access ('Link Following')	16-Nov-2023	7.3	Dell Encryption, Dell Endpoint Security Suite Enterprise, and Dell Security Management Server version prior to 11.8.1 contain an Insecure Operation on Windows Junction Vulnerability during installation. A local malicious user could potentially exploit this vulnerability to create an arbitrary folder inside a restricted directory, leading to Privilege Escalation **CVE ID : CVE-2023-39246**	https://www.dell.com/support/kbdoc/en-us/000217572/dsa-2023-271	A-DEL-SECU-181223/481
Product: unityvsa_operating_environment					
Affected Version(s): * Up to (excluding) 5.3.0.0.5.120					

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 Certificate Validation	22-Nov-2023	5.9	Dell Unity prior to 5.3 contains a 'man in the middle' vulnerability in the vmadapter component. If a customer has a certificate signed by a third-party public Certificate Authority, the vCenter CA could be spoofed by an attacker who can obtain a CA-signed certificate. **CVE ID : CVE-2023-43082**	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-181223/482
Product: unity_operating_environment					
Affected Version(s): * Up to (excluding) 5.3.0.0.5.120					
Improper Certificate Validation	22-Nov-2023	5.9	Dell Unity prior to 5.3 contains a 'man in the middle' vulnerability in the vmadapter component. If a customer has a certificate signed by a third-party public Certificate Authority, the vCenter CA could be spoofed by an attacker who can obtain a CA-signed certificate.	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-181223/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43082		
Product: unity_xt_operating_environment					
Affected Version(s): * Up to (excluding) 5.3.0.0.5.120					
Improper Certificate Validation	22-Nov-2023	5.9	Dell Unity prior to 5.3 contains a 'man in the middle' vulnerability in the vmadapter component. If a customer has a certificate signed by a third-party public Certificate Authority, the vCenter CA could be spoofed by an attacker who can obtain a CA-signed certificate. **CVE ID : CVE-2023-43082**	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-181223/484
Vendor: devolutions					
Product: devolutions_server					
Affected Version(s): * Up to (excluding) 2023.3.8.0					
Exposure of Sensitive Information to an Unauthorized Actor	22-Nov-2023	5.3	Information leak in Content-Security-Policy header in Devolutions Server 2023.3.7.0 allows an unauthenticated attacker to list the configured Devolutions Gateways endpoints.	https://devolutions.net/security/advisories/DEVO-2023-0020/	A-DEV-DEVO-181223/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6264		
Vendor: dguzun					
Product: article_analytics					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Nov-2023	9.8	The Article Analytics WordPress plugin does not properly 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 vulnerability. **CVE ID : CVE-2023-5640**	N/A	A-DGU-ARTI-181223/486
Vendor: diywebmastery					
Product: footer_putter					
Affected Version(s): * Up to (including) 1.17					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Russell Jamieson Footer Putter plugin <= 1.17 versions.	N/A	A-DIY-FOOT-181223/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47768		
Vendor: drd					
Product: drdrive					
Affected Version(s): * Up to (excluding) 2023.10.06					
N/A	22-Nov-2023	0	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in DRD Fleet Leasing DRDrive allows SQL Injection.This issue affects DRDrive: before 20231006. **CVE ID : CVE-2023-5047**	N/A	A-DRD-DRDR-181223/488
Vendor: dreamer_cms_project					
Product: dreamer_cms					
Affected Version(s): 4.1.3					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Dreamer_cms 4.1.3 is vulnerable to Cross Site Request Forgery (CSRF) via Add permissions to CSRF in Permission Management. **CVE ID : CVE-2023-48017**	N/A	A-DRE-DREA-181223/489
Vendor: drelton					
Product: medialist					
Affected Version(s): * Up to (excluding) 1.4.1					
Improper Neutralizat	27-Nov-2023	5.4	The Medialist WordPress plugin	N/A	A-DRE-MEDI-181223/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			before 1.4.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-5942**		
Vendor: droitthemes					
Product: droit_dark_mode					
Affected Version(s): * Up to (including) 1.1.2					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in DroitThemes Droit Dark Mode.This issue affects Droit Dark Mode: from n/a through 1.1.2. **CVE ID : CVE-2023-47531**	N/A	A-DRO-DROI-181223/491
Vendor: duetdisplay					
Product: duet_display					
Affected Version(s): 2.5.9.1					
N/A	21-Nov-2023	7.8	An uncontrolled search path element vulnerability has	N/A	A-DUE-DUET-181223/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been found in the Duet Display product, affecting version 2.5.9.1. An attacker could place an arbitrary libusk.dll file in the C:\Users\user\AppData\Local\Microsoft\WindowsApps\ directory, which could lead to the execution and persistence of arbitrary code. **CVE ID : CVE-2023-6235**		
Vendor: dwuser					
Product: easyrotator_for_wordpress					
Affected Version(s): * Up to (including) 1.0.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	The EasyRotator for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'easyrotator' shortcode in all versions up to, and including, 1.0.14 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level	https://plugins.trac.wordpress.org/browser/easyrotator-for-wordpress/tags/1.0.14/easyrotator.php#L1913	A-DWU-EASY-181223/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5742**		
Vendor: Elastic					
Product: elasticsearch					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.17.14					
Improper Handling of Exceptional Conditions	22-Nov-2023	7.5	It was identified that malformed scripts used in the script processor of an Ingest Pipeline could cause an Elasticsearch node to crash when calling the Simulate Pipeline API. **CVE ID : CVE-2023-46673**	https://discuss.elastic.co/t/elasticsearch-7-17-14-8-10-3-security-update-esa-2023-24/347708, https://www.elastic.co/community/security	A-ELA-ELAS-181223/494
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.10.3					
Improper Handling of Exceptional Conditions	22-Nov-2023	7.5	It was identified that malformed scripts used in the script processor of an Ingest Pipeline could cause an Elasticsearch node to crash when calling the Simulate Pipeline API. **CVE ID : CVE-2023-46673**	https://discuss.elastic.co/t/elasticsearch-7-17-14-8-10-3-security-update-esa-2023-24/347708, https://www.elastic.co/community/security	A-ELA-ELAS-181223/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: epiph					
Product: embed_privacy					
Affected Version(s): * Up to (excluding) 1.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	5.4	The `Embed Privacy` plugin for WordPress that prevents the loading of embedded external content is vulnerable to Stored Cross-Site Scripting via `embed_privacy_opt_out` shortcode in versions up to, and including, 1.8.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Version 1.8.1 contains a patch for this issue. **CVE ID : CVE-2023-48300**	https://github.com/epiphyt/embed-privacy/security/advisories/GHSA-3wv9-4rvf-w37g, https://github.com/epiphyt/embed-privacy/commit/f80929992b2a5a66f4f4953cd6f46cc227154a5c	A-EPI-EMBE-181223/496
Vendor: exeebit					
Product: phpinfo\(\)_wp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 4.0					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Exeebit phpinfo() WP plugin <= 4.0 versions. **CVE ID : CVE-2023-26542**	N/A	A-EXE-PHPI-181223/497
Vendor: eyoucms					
Product: eyoucms					
Affected Version(s): 1.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	eyoucms v1.6.4 is vulnerable Cross Site Scripting (XSS), which can lead to stealing sensitive information of logged-in users. **CVE ID : CVE-2023-46935**	N/A	A-EYO-EYOU-181223/498
Vendor: F5					
Product: big-ip_global_traffic_manager					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/500
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/501
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update	N/A	A-F5-BIG--181223/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			messages containing a malformed attribute. **CVE ID : CVE-2023-45886**		
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/503
Product: big-ip_local_traffic_manager					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/504
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/505
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.10					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/506
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.4					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages	N/A	A-F5-BIG--181223/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing a malformed attribute. **CVE ID : CVE-2023-45886**		
Affected Version(s): From (including) 17.1.0 Up to (including) 17.1.1					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/508
Product: big-ip_next					
Affected Version(s): 20.0.1					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/509
Product: big-ip_next_cloud-native_network_functions					
Affected Version(s): From (including) 1.1.0 Up to (including) 1.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/510
Product: big-ip_next_service_proxy_for_kubernetes					
Affected Version(s): From (including) 1.5.0 Up to (including) 1.8.2					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-F5-BIG--181223/511
Vendor: Ffmpeg					
Product: ffmpeg					
Affected Version(s): * Up to (excluding) 6.1					
Out-of-bounds Write	16-Nov-2023	7.8	Buffer Overflow vulnerability in Ffmpeg before github commit 4565747056a11356210ed8edcecb920	https://github.com/FFmpeg/FFmpeg/commit/4565747056a11356210ed8edcecb920105e	A-FFM-FFMP-181223/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			105e40b60 allows a remote attacker to achieve an out-of-array write, execute arbitrary code, and cause a denial of service (DoS) via the ref_pic_list_struct function in libavcodec/evc_ps.c **CVE ID : CVE-2023-47470**	40b60, https://github.com/goldds96/Report/tree/main/FFmpeg	
Vendor: fivestarplugins					
Product: five_star_restaurant_menu					
Affected Version(s): * Up to (excluding) 2.4.11					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Nov-2023	9.8	The Five Star Restaurant Menu and Food Ordering WordPress plugin before 2.4.11 unserializes user input via an AJAX action available to unauthenticated users, allowing them to perform PHP Object Injection when a suitable gadget is present on the blog. **CVE ID : CVE-2023-5340**	N/A	A-FIV-FIVE-181223/513
Vendor: fla-shop					
Product: interactive_world_map					
Affected Version(s): * Up to (including) 3.2.0					
Improper Neutralization of Input During	22-Nov-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site	N/A	A-FLA-INTE-181223/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting') vulnerability in Fla-shop.Com Interactive World Map plugin <= 3.2.0 versions. **CVE ID : CVE-2023-47767**		
Vendor: fluenx					
Product: deepl_pro_api_translation					
Affected Version(s): * Up to (including) 2.1.4					
N/A	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Fluenx DeepL API translation plugin <= 2.1.4 versions. **CVE ID : CVE-2023-27446**	N/A	A-FLU-DEEP-181223/515
Vendor: fortra					
Product: digital_guardian_agent					
Affected Version(s): * Up to (excluding) 7.9.4					
Insecure Storage of Sensitive Informatio n	22-Nov-2023	6	A saved encryption key in the Uninstaller in Digital Guardian's Agent before version 7.9.4 allows a local attacker to retrieve the uninstall key and remove the software by extracting the uninstaller key from the memory of the uninstaller file.	N/A	A-FOR-DIGI-181223/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6253		
Vendor: free5gc					
Product: free5gc					
Affected Version(s): 3.3.0					
Uncontrolled Resource Consumption	16-Nov-2023	5.5	An issue in Free5gc v.3.3.0 allows a local attacker to cause a denial of service via the free5gc-compose component. **CVE ID : CVE-2023-47025**	N/A	A-FRE-FREE-181223/517
Vendor: fujielectric					
Product: tellus_lite_v-simulator					
Affected Version(s): * Up to (excluding) 4.0.19.0					
N/A	22-Nov-2023	8.8	A user with a standard account in Fuji Electric Tellus Lite may overwrite files in the system. **CVE ID : CVE-2023-5299**	https://felib.fujielectric.co.jp/en/M10009/M20034/document_detail/c27d5b69-68ef-4af5-90ee-b5dab118f71a	A-FUJ-TELL-181223/518
Out-of-bounds Write	22-Nov-2023	7.8	Stack-based buffer overflow may occur when Fuji Electric Tellus Lite V-Simulator parses a specially-crafted input file. **CVE ID : CVE-2023-35127**	https://felib.fujielectric.co.jp/en/M10009/M20034/document_detail/c27d5b69-68ef-4af5-90ee-b5dab118f71a	A-FUJ-TELL-181223/519
Out-of-bounds Write	22-Nov-2023	7.8	When Fuji Electric Tellus Lite V-Simulator parses a specially-crafted input file an out of	https://felib.fujielectric.co.jp/en/M10009/M20034/document_detail/c27d5b69-68ef-4af5-	A-FUJ-TELL-181223/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds write may occur. **CVE ID : CVE-2023-40152**	90ee-b5dab118f71a	
Vendor: funnelforms					
Product: funnelforms					
Affected Version(s): * Up to (including) 3.4					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	4.3	The Funnelforms Free plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.4. This is due to missing or incorrect nonce validation on the fnsf_delete_posts function. This makes it possible for unauthenticated attackers to delete arbitrary posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-5382**	https://plugins.trac.wordpress.org/changeset/2986938/funnelforms-free	A-FUN-FUNN-181223/521
Cross-Site Request Forgery (CSRF)	22-Nov-2023	4.3	The Funnelforms Free plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.4. This is due to missing or	https://plugins.trac.wordpress.org/changeset/2986938/funnelforms-free	A-FUN-FUNN-181223/522

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
			incorrect nonce validation on the fnsf_copy_posts function. This makes it possible for unauthenticated attackers to create copies of arbitrary posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-5383**		
Missing Authorization	22-Nov-2023	4.3	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_copy_posts function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to create copies of arbitrary posts. **CVE ID : CVE-2023-5385**	https://plugins.trac.wordpress.org/changeset/2986938/funnelforms-free	A-FUN-FUNN-181223/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	22-Nov-2023	4.3	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_delete_posts function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete arbitrary posts, including administrator posts, and posts not related to the Funnelforms Free plugin. **CVE ID : CVE-2023-5386**	https://plugins.trac.wordpress.org/changeset/2986938/funnelforms-free	A-FUN-FUNN-181223/524
Missing Authorization	22-Nov-2023	4.3	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_af2_trigger_dark_mode function in versions up to, and including, 3.4. This makes it possible for authenticated	https://plugins.trac.wordpress.org/changeset/2986938/funnelforms-free	A-FUN-FUNN-181223/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers, with subscriber-level permissions and above, to enable or disable the dark mode plugin setting. **CVE ID : CVE-2023-5387**		
Missing Authorization	22-Nov-2023	4.3	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_af2_save_post function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to modify certain post values. Note that the extent of modification is limited due to fixed values passed to the wp_update_post function. **CVE ID : CVE-2023-5411**	https://plugins.trac.wordpress.org/changeset/2986938/funnelforms-free	A-FUN-FUNN-181223/526
Missing Authorization	22-Nov-2023	4.3	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of	https://plugins.trac.wordpress.org/changeset/2986938/funnelforms-free	A-FUN-FUNN-181223/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data due to a missing capability check on the fnsf_add_category function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to add new categories. **CVE ID : CVE-2023-5415**		
Missing Authorization	22-Nov-2023	4.3	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_delete_category function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete categories. **CVE ID : CVE-2023-5416**	https://plugins.trac.wordpress.org/changeset/2986938/funnelforms-free	A-FUN-FUNN-181223/528
Missing Authorization	22-Nov-2023	4.3	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized	https://plugins.trac.wordpress.org/changeset	A-FUN-FUNN-181223/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modification of data due to a missing capability check on the fnsf_update_category function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to modify the Funnelforms category for a given post ID. **CVE ID : CVE-2023-5417**	/2986938/funnelforms-free	
Missing Authorization	22-Nov-2023	4.3	The Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the fnsf_af2_test_mail function in versions up to, and including, 3.4. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to send test emails to an arbitrary email address. **CVE ID : CVE-2023-5419**	https://plugins.trac.wordpress.org/changeset/2986938/funnelforms-free	A-FUN-FUNN-181223/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Get-simple					
Product: getsimplecms					
Affected Version(s): 3.3.16					
Improper Control of Generation of Code ('Code Injection')	17-Nov-2023	9.8	A vulnerability was found in GetSimpleCMS 3.3.16/3.4.0a. It has been rated as critical. This issue affects some unknown processing of the file /admin/theme-edit.php. The manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-245735. **CVE ID : CVE-2023-6188**	N/A	A-GET-GETS-181223/531
Affected Version(s): 3.4.0a					
Improper Control of Generation of Code ('Code Injection')	17-Nov-2023	9.8	A vulnerability was found in GetSimpleCMS 3.3.16/3.4.0a. It has been rated as critical. This issue affects some unknown processing of the file /admin/theme-edit.php. The manipulation leads to code injection.	N/A	A-GET-GETS-181223/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-245735. **CVE ID : CVE-2023-6188**		
Vendor: getgrav					
Product: dom-sanitizer					
Affected Version(s): * Up to (excluding) 1.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	6.1	DOMSanitizer (aka dom-sanitizer) before 1.0.7 allows XSS via an SVG document because of mishandling of comments and greedy regular expressions. **CVE ID : CVE-2023-49146**	https://github.com/rhukster/dom-sanitizer/commit/c2a98f27ad742668b254282ccc5581871d0fb601, https://github.com/rhukster/dom-sanitizer/compare/1.0.6...1.0.7	A-GET-DOM--181223/533
Vendor: ggnome					
Product: garden_gnome_package					
Affected Version(s): * Up to (excluding) 2.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	The Garden Gnome Package plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ggpkg' shortcode in all versions up to, and including, 2.2.8 due	https://plugins.trac.wordpress.org/browser/garden-gnome-package/tags/2.2.5/include/ggpackage.php#L284, https://plugins.trac.wordpress	A-GGN-GARD-181223/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This was partially patched in version 2.2.7 and fully patched in version 2.2.9. **CVE ID : CVE-2023-5664**	.org/changeset/2987987/garden-gnome-package#file1	
Vendor: giflib_project					
Product: giflib					
Affected Version(s): 5.2.1					
Out-of-bounds Write	22-Nov-2023	7.1	Buffer Overflow vulnerability in GifLib Project GifLib v.5.2.1 allows a local attacker to obtain sensitive information via the DumpSCreen2RGB function in gif2rgb.c **CVE ID : CVE-2023-48161**	N/A	A-GIF-GIFL-181223/535
Vendor: git-urls_project					
Product: git-urls					
Affected Version(s): 1.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Nov-2023	7.5	git-urls 1.0.0 allows ReDOS (Regular Expression Denial of Service) in urls.go. **CVE ID : CVE-2023-46402**	N/A	A-GIT-GIT--181223/536
Vendor: glewlwyd_sso_server_project					
Product: glewlwyd_sso_server					
Affected Version(s): * Up to (excluding) 2.7.6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Nov-2023	9.8	scheme/webauthn.c in Glewlwyd SSO server before 2.7.6 has a possible buffer overflow during FIDO2 credentials validation in webauthn registration. **CVE ID : CVE-2023-49208**	https://github.com/babelouest/glewlwyd/commit/f9d8c06aae8dfe17e761b18b577ff169e059e812, https://github.com/babelouest/glewlwyd/releases/tag/v2.7.6	A-GLE-GLEW-181223/537
Vendor: goauthentik					
Product: authentik					
Affected Version(s): * Up to (excluding) 2023.8.5					
N/A	21-Nov-2023	9.8	authentik is an open-source identity provider. When initialising a oauth2 flow with a `code_challenge` and `code_method` (thus requesting PKCE), the single sign-on provider (authentik) must check if there is a matching and existing `code_verifier` during the token	https://github.com/goauthentik/authentik/security/advisories/GHSA-fm34-v8xq-f2c3, https://github.com/goauthentik/authentik/pull/7666, https://github.com/goauthentik/authentik/pull/7668, https://github.	A-GOA-AUTH-181223/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			step. Prior to versions 2023.10.4 and 2023.8.5, authentik checks if the contents of `code_verifier` is matching only when it is provided. When it is left out completely, authentik simply accepts the token request with out it; even when the flow was started with a `code_challenge`. authentik 2023.8.5 and 2023.10.4 fix this issue. **CVE ID : CVE-2023-48228**	com/goauthentik/authentik/pull/7669	
Affected Version(s): From (including) 2023.10.0 Up to (excluding) 2023.10.4					
N/A	21-Nov-2023	9.8	authentik is an open-source identity provider. When initialising a oauth2 flow with a `code_challenge` and `code_method` (thus requesting PKCE), the single sign-on provider (authentik) must check if there is a matching and existing `code_verifier` during the token step. Prior to versions 2023.10.4 and 2023.8.5, authentik checks if the contents of	https://github.com/goauthentik/authentik/security/advisories/GHSA-fm34-v8xq-f2c3, https://github.com/goauthentik/authentik/pull/7666, https://github.com/goauthentik/authentik/pull/7668, https://github.com/goauthentik/authentik/pull/7669	A-GOA-AUTH-181223/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`code_verifier` is matching only when it is provided. When it is left out completely, authentik simply accepts the token request with out it; even when the flow was started with a `code_challenge`. authentik 2023.8.5 and 2023.10.4 fix this issue. **CVE ID : CVE-2023-48228**		
Vendor: gopiplus					
Product: popup_with_fancybox					
Affected Version(s): * Up to (including) 3.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Nov-2023	8.8	The Popup with fancybox plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 3.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional	https://plugins.trac.wordpress.org/browser/popup-with-fancybox/trunk/popup-with-fancybox.php?rev=2827070#L110, https://plugins.trac.wordpress.org/changeset/2985560/popup-with-fancybox#file1	A-GOP-POPU-181223/540

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 queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5465**		
Product: vertical_scroll_recent_registered_user					
Affected Version(s): * Up to (including) 9.1					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Gopi Ramasamy Vertical scroll recent.This issue affects Vertical scroll recent post: from n/a through 14.0. **CVE ID : CVE-2023-47671**	N/A	A-GOP-VERT-181223/541
Product: wp_anything_slider					
Affected Version(s): * Up to (including) 9.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Nov-2023	8.8	The Wp anything slider plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 9.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the	https://plugins.trac.wordpress.org/browser/wp-anything-slider/trunk/wp-anything-slider.php?rev=2827063#L122 , https://plugins.trac.wordpress.org/browser/wp-anything-slider/trunk/w	A-GOP-WP_A-181223/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-5466**	p-anything-slider.php?rev=2827063#L136	
Vendor: gowebsolutions					
Product: wp_customer_reviews					
Affected Version(s): * Up to (including) 3.6.6					
N/A	22-Nov-2023	4.3	The WP Customer Reviews plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 3.6.6 via the ajax_enabled_posts function. This can allow authenticated attackers to extract sensitive data such as post titles and slugs, including those of protected and trashed posts and pages in addition to other	https://plugins.trac.wordpress.org/changeset/2965656/wp-customer-reviews/trunk?contextall=1&old=2882143&old_path=%2Fwp-customer-reviews%2Ftrunk	A-GOW-WP_C-181223/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			post types such as galleries. **CVE ID : CVE-2023-4686**		
Vendor: gpac					
Product: gpac					
Affected Version(s): 2.3-dev-rev617-g671976fcc-master					
Missing Release of Memory after Effective Lifetime	20-Nov-2023	7.1	GPAC 2.3-DEV-rev617-g671976fcc-master is vulnerable to memory leaks in extract_attributes media_tools/m3u8.c:329. **CVE ID : CVE-2023-48090**	https://github.com/gpac/gpac/issues/2680	A-GPA-GPAC-181223/544
Missing Release of Memory after Effective Lifetime	20-Nov-2023	5.5	GPAC 2.3-DEV-rev617-g671976fcc-master is vulnerable to memory leak in gf_mpd_parse_string media_tools/mpd.c:75. **CVE ID : CVE-2023-48039**	https://github.com/gpac/gpac/issues/2679	A-GPA-GPAC-181223/545
Vendor: grandslambert					
Product: better_rss_widget					
Affected Version(s): * Up to (including) 2.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in grandslambert Better RSS Widget	N/A	A-GRA-BETT-181223/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin <= 2.8.1 versions. **CVE ID : CVE-2023-47813**		
Vendor: grupoalumne					
Product: alumne_lms					
Affected Version(s): 4.0.0.1.08					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Nov-2023	6.1	A Cross-Site Scripting (XSS) vulnerability has been found in Alumne LMS affecting version 4.0.0.1.08. An attacker could exploit the 'localidad' parameter to inject a custom JavaScript payload and partially take over another user's browser session, due to the lack of proper sanitisation of the 'localidad' field on the /users/editmy page. **CVE ID : CVE-2023-6359**	N/A	A-GRU-ALUM-181223/547
Vendor: gvectors					
Product: wpdiscuz					
Affected Version(s): * Up to (excluding) 7.6.12					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in gVectors Team Comments —	N/A	A-GVE-WPDI-181223/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wpDiscuz plugin <= 7.6.11 versions. **CVE ID : CVE-2023-47775**		
Vendor: h-mdm					
Product: headwind_mdm					
Affected Version(s): 5.22.1					
Use of Hard-coded Credentials	22-Nov-2023	8.8	Headwind MDM Web panel 5.22.1 is vulnerable to Incorrect Access Control due to a hard-coded JWT Secret. The secret is hardcoded into the source code available to anyone on Git Hub. This secret is used to sign the application's JWT token and verify the incoming user-supplied tokens. **CVE ID : CVE-2023-47315**	N/A	A-H-M-HEAD-181223/549
Cleartext Storage of Sensitive Information	22-Nov-2023	6.5	Headwind MDM Web panel 5.22.1 is vulnerable to Incorrect Access Control due to Login Credential Leakage via Audit Entries. **CVE ID : CVE-2023-47312**	N/A	A-H-M-HEAD-181223/550
Improper Limitation of a Pathname to a	22-Nov-2023	5.4	Headwind MDM Web panel 5.22.1 is vulnerable to Directory Traversal. The	N/A	A-H-M-HEAD-181223/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			application uses an API call to move the uploaded temporary file to the file directory during the file upload process. This API call receives two input parameters, such as path and localPath. The first one refers to the temporary file with an absolute path without validating it. Attackers may modify this API call by referring to arbitrary files. As a result, arbitrary files can be moved to the files directory and so they can be downloaded. **CVE ID : CVE-2023-47313**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Headwind MDM Web panel 5.22.1 is vulnerable to cross-site scripting (XSS). The file upload function allows APK and arbitrary files to be uploaded. By exploiting this issue, attackers may upload HTML files and share the download URL pointing to these files with the	N/A	A-H-M-HEAD-181223/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victims. As the file download function returns the file in inline mode, the victim's browser will immediately render the content of the HTML file as a web page. As a result, the uploaded client-side code will be evaluated and executed in the victim's browser, allowing attackers to perform common XSS attacks. **CVE ID : CVE-2023-47314**		
Authorization Bypass Through User-Controlled Key	22-Nov-2023	5.4	Headwind MDM Web panel 5.22.1 is vulnerable to Incorrect Access Control. The Web panel allows users to gain access to potentially sensitive API calls such as listing users and their data, file management API calls and audit-related API calls. **CVE ID : CVE-2023-47316**	N/A	A-H-M-HEAD-181223/553
Vendor: h2o					
Product: h2o					
Affected Version(s): -					
N/A	16-Nov-2023	9.8	An attacker is able to gain remote code execution on a	N/A	A-H2O-H2O-181223/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server hosting the H2O dashboard through it's POJO model import feature. **CVE ID : CVE-2023-6016**		
Missing Authorization	16-Nov-2023	7.5	An attacker is able to read any file on the server hosting the H2O dashboard without any authentication. **CVE ID : CVE-2023-6038**	N/A	A-H2O-H2O-181223/555
N/A	16-Nov-2023	7.1	H2O included a reference to an S3 bucket that no longer existed allowing an attacker to take over the S3 bucket URL. **CVE ID : CVE-2023-6017**	N/A	A-H2O-H2O-181223/556
N/A	16-Nov-2023	5.4	H2O is vulnerable to stored XSS vulnerability which can lead to a Local File Include attack. **CVE ID : CVE-2023-6013**	N/A	A-H2O-H2O-181223/557
Vendor: Hikvision					
Product: localservicecomponents					
Affected Version(s): * Up to (including) 1.0.0.78					
Buffer Copy without Checking Size of	23-Nov-2023	9.8	There is a buffer overflow vulnerability in a web browser plug-in could allow an	https://www.hikvision.com/en/support/cybersecurity/security-	A-HIK-LOCA-181223/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			attacker to exploit the vulnerability by sending crafted messages to computers installed with this plug-in, which could lead to arbitrary code execution or cause process exception of the plug-in. **CVE ID : CVE-2023-28812**	advisory/security-vulnerabilities-in-hikvision-web-browser-plug-in-locals/	
N/A	23-Nov-2023	7.5	An attacker could exploit a vulnerability by sending crafted messages to computers installed with this plug-in to modify plug-in parameters, which could cause affected computers to download malicious files. **CVE ID : CVE-2023-28813**	https://www.hikvision.com/en/support/cybersecurity/security-advisory/security-vulnerabilities-in-hikvision-web-browser-plug-in-locals/	A-HIK-LOCA-181223/559
Vendor: himanshuparashar					
Product: google_site_verification_plugin_using_meta_tag					
Affected Version(s): * Up to (including) 1.2					
N/A	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Himanshu Parashar Google Site Verification plugin using Meta Tag.This issue affects Google Site Verification plugin using Meta	N/A	A-HIM-GOOG-181223/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tag: from n/a through 1.2. **CVE ID : CVE-2023-32514**		
Vendor: Honeywell					
Product: prowatch					
Affected Version(s): 4.5					
Incorrect Permission Assignment for Critical Resource	17-Nov-2023	7.8	Honeywell ProWatch, 4.5, including all Service Pack versions, contain a Vulnerability in Application Server's executable folder(s). A(n) attacker could potentially exploit this vulnerability, leading to a standard user to have arbitrary system code execution. Honeywell recommends updating to the most recent version of this product, service or offering (Pro-watch 6.0.2, 6.0, 5.5.2,5.0.5). **CVE ID : CVE-2023-6179**	N/A	A-HON-PROW-181223/561
Vendor: howerj					
Product: liblisp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2019-02-08					
Out-of-bounds Read	17-Nov-2023	8.1	Liblisp through commit 4c65969 was discovered to contain a out-of-bounds-read vulnerability in unsigned get_length(lisp_cell_t * x) at eval.c **CVE ID : CVE-2023-48025**	N/A	A-HOW-LIBL-181223/562
Use After Free	17-Nov-2023	6.5	Liblisp through commit 4c65969 was discovered to contain a use-after-free vulnerability in void hash_destroy(hash_table_t *h) at hash.c **CVE ID : CVE-2023-48024**	N/A	A-HOW-LIBL-181223/563
Vendor: httpie					
Product: httpie					
Affected Version(s): 3.2.2					
Improper Certificate Validation	16-Nov-2023	7.4	Missing SSL certificate validation in HTTPie v3.2.2 allows attackers to eavesdrop on communications between the host and server via a man-in-the-middle attack. **CVE ID : CVE-2023-48052**	N/A	A-HTT-HTTP-181223/564
Vendor: hyphensolutions					
Product: chameleon_power					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-2023	7.5	Path traversal vulnerability in Chalemelon Power framework, affecting the getImage parameter. This vulnerability could allow a remote user to read files located on the server and gain access to sensitive information such as configuration files. **CVE ID : CVE-2023-6252**	N/A	A-HYP-CHAM-181223/565
Vendor: IBM					
Product: cics_tx					
Affected Version(s): 10.1					
N/A	18-Nov-2023	7.5	IBM CICS TX Advanced 10.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 260770. **CVE ID : CVE-2023-38361**	https://www.ibm.com/support/pages/node/7066431, https://exchange.xforce.ibmcloud.com/vulnerabilities/260770	A-IBM-CICS-181223/566
Product: infosphere_information_server					
Affected Version(s): 11.7					
Incorrect Default	18-Nov-2023	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user	https://exchange.xforce.ibmcloud.com/vulne	A-IBM-INFO-181223/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			to change installation files due to incorrect file permission settings. IBM X-Force ID: 263332. **CVE ID : CVE-2023-40363**	rabilities/263332	
Product: qradar_wincollect					
Affected Version(s): From (including) 10.0 Up to (including) 10.1.7					
Improper Encoding or Escaping of Output	24-Nov-2023	7.8	IBM QRadar WinCollect Agent 10.0 through 10.1.7 could allow a local user to perform unauthorized actions due to improper encoding. IBM X-Force ID: 248160. **CVE ID : CVE-2023-26279**	https://www.ibm.com/support/pages/node/7081403, https://exchange.xforce.ibmcloud.com/vulnerabilities/213551	A-IBM-QRAD-181223/568
Product: sterling_b2b_integrator					
Affected Version(s): From (including) 6.0.0.0 Up to (excluding) 6.0.3.9					
Insertion of Sensitive Information into Log File	22-Nov-2023	5.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.1 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 247034.	https://www.ibm.com/support/pages/node/7080172, https://exchange.xforce.ibmcloud.com/vulnerabilities/247034	A-IBM-STER-181223/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25682		
Affected Version(s): From (including) 6.1.0.0 Up to (excluding) 6.1.2.3					
Insertion of Sensitive Information into Log File	22-Nov-2023	5.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.1 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 247034. **CVE ID : CVE-2023-25682**	https://www.ibm.com/support/pages/node/7080172, https://exchange.xforce.ibmcloud.com/vulnerabilities/247034	A-IBM-STER-181223/570
Vendor: icansoft					
Product: korea_sns					
Affected Version(s): * Up to (including) 1.6.3					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Jongmyoung Kim Korea SNS.This issue affects Korea SNS: from n/a through 1.6.3. **CVE ID : CVE-2023-47670**	N/A	A-ICA-KORE-181223/571
Vendor: ifeelweb					
Product: post_status_notifier_lite					
Affected Version(s): * Up to (excluding) 1.11.1					
Improper Neutralization of	22-Nov-2023	6.1	Improper Neutralization of Input During Web	N/A	A-IFE-POST-181223/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Page Generation ('Cross-site Scripting') vulnerability in Timo Reith Post Status Notifier Lite plugin <= 1.11.0 versions. **CVE ID : CVE-2023-47766**		
Vendor: implecode					
Product: ecommerce_product_catalog					
Affected Version(s): * Up to (including) 3.3.26					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in impleCode eCommerce Product Catalog Plugin for WordPress plugin <= 3.3.26 versions. **CVE ID : CVE-2023-47839**	N/A	A-IMP-ECOM-181223/573
Vendor: incsub					
Product: forminator					
Affected Version(s): * Up to (excluding) 1.27.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	4.8	The Forminator WordPress plugin before 1.27.0 does not properly sanitize the redirect-url field in the form submission settings, which could allow high-	N/A	A-INC-FORM-181223/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege users such as an administrator to inject arbitrary web scripts even when the unfiltered_html capability is disallowed (for example in a multisite setup). **CVE ID : CVE-2023-5119**		
Vendor: infiniteuploads					
Product: big_file_uploads					
Affected Version(s): * Up to (excluding) 2.1.2					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Infinite Uploads Big File Uploads – Increase Maximum File Upload Size plugin <= 2.1.1 versions. **CVE ID : CVE-2023-47792**	N/A	A-INF-BIG_-181223/575
Vendor: infornweb					
Product: news_\&_blog_designer_pack					
Affected Version(s): * Up to (including) 3.4.1					
N/A	22-Nov-2023	9.8	The News & Blog Designer Pack – WordPress Blog Plugin — (Blog Post Grid, Blog Post Slider, Blog Post Carousel, Blog Post Ticker, Blog Post Masonry) plugin for WordPress is vulnerable to Remote Code	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2984052%40blog-designer-pack&new=2984052%40blog-designer-	A-INF-NEWS-181223/576

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
			Execution via Local File Inclusion in all versions up to, and including, 3.4.1 via the bdp_get_more_post function hooked via a nopriv AJAX. This is due to function utilizing an unsafe extract() method to extract values from the POST variable and passing that input to the include() function. This makes it possible for unauthenticated attackers to include arbitrary PHP files and achieve remote code execution. On vulnerable Docker configurations it may be possible for an attacker to create a PHP file and then subsequently include it to achieve RCE. **CVE ID : CVE-2023-5815**	pack&sfp_email=&sfph_mail=	
Vendor: ioannup					
Product: edit_woocommerce_templates					
Affected Version(s): * Up to (including) 1.1.1					
Improper Neutralization of Input During	16-Nov-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ioannup Edit WooCommerce	N/A	A-IOA-EDIT-181223/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Templates plugin <= 1.1.1 versions. **CVE ID : CVE-2023-47509**		
Vendor: ipinfusion					
Product: zebos					
Affected Version(s): * Up to (including) 7.10.6					
N/A	21-Nov-2023	7.5	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute. **CVE ID : CVE-2023-45886**	N/A	A-IPI-ZEBO-181223/578
Vendor: ironmansoftware					
Product: powershell_universal					
Affected Version(s): 4.2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Nov-2023	8.8	The API endpoints in Ironman PowerShell Universal 3.0.0 through 4.2.0 allow remote attackers to execute arbitrary commands via crafted HTTP requests if a param block is used, due to invalid sanitization of input strings. The fixed versions are	https://blog.ironmansoftware.com/powershell-universal-apis-cve/	A-IRO-POWE-181223/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.10.2, 4.1.10, and 4.2.1. **CVE ID : CVE-2023-49213**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.10.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Nov-2023	8.8	The API endpoints in Ironman PowerShell Universal 3.0.0 through 4.2.0 allow remote attackers to execute arbitrary commands via crafted HTTP requests if a param block is used, due to invalid sanitization of input strings. The fixed versions are 3.10.2, 4.1.10, and 4.2.1. **CVE ID : CVE-2023-49213**	https://blog.ironmansoftware.com/powershell-universal-apis-cve/	A-IRO-POWE-181223/580
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.10					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Nov-2023	8.8	The API endpoints in Ironman PowerShell Universal 3.0.0 through 4.2.0 allow remote attackers to execute arbitrary commands via crafted HTTP requests if a param block is used, due to invalid sanitization of input strings. The fixed versions are 3.10.2, 4.1.10, and 4.2.1.	https://blog.ironmansoftware.com/powershell-universal-apis-cve/	A-IRO-POWE-181223/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49213		
Vendor: itextpdf					
Product: itext					
Affected Version(s): 8.0.1					
Missing Release of Memory after Effective Lifetime	26-Nov-2023	6.5	A vulnerability, which was classified as problematic, has been found in Apryse iText 8.0.1. This issue affects some unknown processing of the file PdfDocument.java of the component Reference Table Handler. The manipulation leads to memory leak. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 8.0.2 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-246125 was assigned to this vulnerability. NOTE: The vendor was contacted early about this vulnerability. The fix was introduced	N/A	A-ITE-ITEX-181223/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the iText 8.0.2 release on October 25th 2023, prior to the disclosure. **CVE ID : CVE-2023-6299**		
Affected Version(s): 8.0.2					
Improper Validation of Array Index	26-Nov-2023	6.5	A vulnerability classified as problematic was found in Apryse iText 8.0.2. This vulnerability affects the function main of the file PdfDocument.java. The manipulation leads to improper validation of array index. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-246124. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-6298**	N/A	A-ITE-ITEX-181223/583
Vendor: jamesmehorter					
Product: device_theme_switcher					
Affected Version(s): * Up to (including) 3.0.2					
Cross-Site Request	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF)	N/A	A-JAM-DEVI-181223/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			vulnerability in James Mehorter Device Theme Switcher.This issue affects Device Theme Switcher: from n/a through 3.0.2. **CVE ID : CVE-2023-47556**		
Vendor: jannisthuemmig					
Product: email_encoder					
Affected Version(s): * Up to (including) 2.1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jannis Thuemmig Email Encoder plugin <= 2.1.8 versions. **CVE ID : CVE-2023-47821**	N/A	A-JAN-EMAI-181223/585
Vendor: jeecg					
Product: jeecg-boot					
Affected Version(s): 3.6.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-2023	6.5	Directory Traversal vulnerability in jeecg-boot v.3.6.0 allows a remote privileged attacker to obtain sensitive information via the file directory structure.	N/A	A-JEE-JEEC-181223/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47467		
Vendor: joaquimserafim					
Product: json_web_token					
Affected Version(s): * Up to (excluding) 3.1.1					
N/A	17-Nov-2023	7.5	joaquimserafim/json-web-token is a javascript library use to interact with JSON Web Tokens (JWT) which are a compact URL-safe means of representing claims to be transferred between two parties. Affected versions of the json-web-token library are vulnerable to a JWT algorithm confusion attack. On line 86 of the 'index.js' file, the algorithm to use for verifying the signature of the JWT token is taken from the JWT token, which at that point is still unverified and thus shouldn't be trusted. To exploit this vulnerability, an attacker needs to craft a malicious JWT token containing the HS256 algorithm, signed with the public RSA key of	https://github.com/joaquimserafim/json-web-token/security/advisories/GHSA-4xw9-cx39-r355	A-JOA-JSON-181223/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the victim application. This attack will only work against this library is the RS256 algorithm is in use, however it is a best practice to use that algorithm. **CVE ID : CVE-2023-48238**		
Vendor: jonashjalmarsson					
Product: html_filter_and_csv-file_search					
Affected Version(s): * Up to (excluding) 2.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	The HTML filter and csv-file search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'csvsearch' shortcode in versions up to, and including, 2.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	https://plugins.trac.wordpress.org/changeset/2985200/hk-filter-and-search	A-JON-HTML-181223/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5096		
Vendor: joselazo					
Product: delete_usermeta					
Affected Version(s): * Up to (including) 1.1.2					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	4.3	The Delete Usermeta plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing nonce validation on the delumet_options_page() function. This makes it possible for unauthenticated attackers to remove user meta for arbitrary users via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-5537**	https://plugins.trac.wordpress.org/browser/delete-usermetas/trunk/delete-usermetas.php#L57, https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2979918%40delete-usermetas&new=2979918%40delete-usermetas&sfp_email=&sfph_mail=	A-JOS-DELE-181223/589
Vendor: kaine					
Product: wise_chat					
Affected Version(s): * Up to (including) 3.1.3					
N/A	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Kainex Wise Chat.This issue affects Wise Chat:	N/A	A-KAI-WISE-181223/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a through 3.1.3. **CVE ID : CVE-2023-32504**		
Vendor: kc_group_e-commerce_software_project					
Product: kc_group_e-commerce_software					
Affected Version(s): * Up to (including) 2023-11-23					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KC Group E-Commerce Software allows Reflected XSS.This issue affects E-Commerce Software: through 20231123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-4406**	N/A	A-KC_-KC_G-181223/591
Vendor: Kibokolabs					
Product: arigato_autoresponder_and_newsletter					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.7.2.2					
Cross-Site Request Forgery (CSRF)	16-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Kiboko Labs Arigato Autoresponder and Newsletter plugin <= 2.7.2.2 versions. **CVE ID : CVE-2023-47686**	N/A	A-KIB-ARIG-181223/592
Vendor: Kingsoft					
Product: wps_office					
Affected Version(s): 11.2.0.11537					
Use of Uninitialized Resource	27-Nov-2023	7.8	An uninitialized pointer use vulnerability exists in the functionality of WPS Office 11.2.0.11537 that handles Data elements in an Excel file. A specially crafted malformed file can lead to remote code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2023-31275**	N/A	A-KIN-WPS_-181223/593
Vendor: kodcloud					
Product: kodbox					
Affected Version(s): 1.46.01					
Improper Restriction of Excessive	18-Nov-2023	9.8	kodbox 1.46.01 has a security flaw that enables user enumeration. This	N/A	A-KOD-KODB-181223/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts		🟥	problem is present on the login page, where an attacker can identify valid users based on varying response messages, potentially paving the way for a brute force attack. **CVE ID : CVE-2023-48028**		
Vendor: kreaturamedia					
Product: layerslider					
Affected Version(s): * Up to (excluding) 7.7.10					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in LayerSlider plugin <= 7.7.9 versions. **CVE ID : CVE-2023-47785**	N/A	A-KRE-LAYE-181223/595
Vendor: layer5					
Product: meshery					
Affected Version(s): * Up to (excluding) 0.6.179					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Nov-2023	9.8	A SQL injection vulnerability in Meshery before 0.6.179 allows a remote attacker to obtain sensitive information and execute arbitrary code via the order parameter. **CVE ID : CVE-2023-46575**	https://github.com/meshery/meshery/commit/ffe00967acfe4444a5db08ff3a4cafb9adf6013f, https://github.com/meshery/meshery/compare/v0.6.178...v0.6.179	A-LAY-MESH-181223/596
Vendor: layerslider					
Product: layerslider					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 7.7.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LayerSlider plugin <= 7.7.9 versions. **CVE ID : CVE-2023-47786**	N/A	A-LAY-LAYE-181223/597
Vendor: leadster					
Product: leadster					
Affected Version(s): * Up to (including) 1.1.2					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Leadster plugin <= 1.1.2 versions. **CVE ID : CVE-2023-47791**	N/A	A-LEA-LEAD-181223/598
Vendor: Lesterchan					
Product: wp-useronline					
Affected Version(s): * Up to (excluding) 2.88.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Nov-2023	6.1	The WP-UserOnline WordPress plugin before 2.88.3 does not sanitise and escape the X-Forwarded-For header before outputting its content on the page, which allows unauthenticated users to perform Cross-Site Scripting attacks.	N/A	A-LES-WP-U-181223/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5560		
Vendor: levantoan					
Product: woocommerce_vietnam_checkout					
Affected Version(s): * Up to (excluding) 2.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Nov-2023	6.1	The Woocommerce Vietnam Checkout WordPress plugin before 2.0.6 does not escape the custom shipping phone field no the checkout form leading to XSS **CVE ID : CVE-2023-5325**	N/A	A-LEV-WOOC-181223/600
Vendor: lfprojects					
Product: mlflow					
Affected Version(s): -					
N/A	16-Nov-2023	9.8	An attacker can overwrite any file on the server hosting MLflow without any authentication. **CVE ID : CVE-2023-6018**	N/A	A-LFP-MLFL-181223/601
Affected Version(s): *					
N/A	16-Nov-2023	9.8	An attacker is able to arbitrarily create an account in MLflow bypassing any authentication requirment. **CVE ID : CVE-2023-6014**	N/A	A-LFP-MLFL-181223/602
Affected Version(s): * Up to (excluding) 2.8.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Nov-2023	7.5	MLflow allowed arbitrary files to be PUT onto the server. **CVE ID : CVE-2023-6015**	N/A	A-LFP-MLFL-181223/603
Vendor: librenms					
Product: librenms					
Affected Version(s): * Up to (excluding) 23.11.0					
Improper Restriction of Excessive Authentication Attempts	17-Nov-2023	7.5	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring which includes support for a wide range of network hardware and operating systems. In affected versions the login method has no rate limit. An attacker may be able to leverage this vulnerability to gain access to user accounts. This issue has been addressed in version 23.11.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-46745**	https://github.com/librenms/librenms/security/advisories/GHSA-rq42-58qf-v3qx	A-LIB-LIBR-181223/604
Improper Neutralization of Input During Web Page	17-Nov-2023	5.4	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring which includes support	https://github.com/librenms/librenms/security/advisories/GHSA-8phr-637g-pxrg,	A-LIB-LIBR-181223/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			for a wide range of network hardware and operating systems. Affected versions are subject to a cross site scripting (XSS) vulnerability in the device group popups. This issue has been addressed in commit `faf66035ea` which has been included in release version 23.11.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48295**	https://github.com/librenms/librenms/commit/faf66035ea1f4c1c4f34559b9d0ed40ee4a19f90	
N/A	17-Nov-2023	4.3	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring which includes support for a wide range of network hardware and operating systems. In affected versions of LibreNMS when a user accesses their device dashboard, one request is sent to `graph.php` to access graphs generated on the particular Device. This request can be	https://github.com/librenms/librenms/security/advisories/GHSA-fpq5-4vwm-78x4, https://github.com/librenms/librenms/commit/489978a923ed52aa243d3419889ca298a8a6a7cf	A-LIB-LIBR-181223/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessed by a low privilege user and they can enumerate devices on librenms with their id or hostname. Leveraging this vulnerability a low privilege user can see all devices registered by admin users. This vulnerability has been addressed in commit `489978a923` which has been included in release version 23.11.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48294**		
Vendor: Libtiff					
Product: libtiff					
Affected Version(s): -					
Uncontrolled Resource Consumption	24-Nov-2023	6.5	An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow a remote attacker to cause a denial of service via a craft input with size smaller than 379 KB. **CVE ID : CVE-2023-6277**	https://bugzilla.redhat.com/show_bug.cgi?id=2251311, https://gitlab.com/libtiff/libtiff/-/issues/614, https://gitlab.com/libtiff/libtiff/-/merge_requests/545	A-LIB-LIBT-181223/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Liferay					
Product: liferay_portal					
Affected Version(s): From (including) 7.4.3.94 Up to (including) 7.4.3.95					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-2023	6.1	Reflected cross-site scripting (XSS) vulnerability on a content page's edit page in Liferay Portal 7.4.3.94 through 7.4.3.95 allows remote attackers to inject arbitrary web script or HTML via the `p_l_back_url_title` parameter. **CVE ID : CVE-2023-47797**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-47797	A-LIF-LIFE-181223/608
Vendor: lifterlms					
Product: lifterlms					
Affected Version(s): * Up to (including) 7.4.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-2023	6.7	The LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 7.4.2 via the maybe_serve_export function. This makes it possible for authenticated attackers, with administrator or LMS manager access and above, to read the contents	N/A	A-LIF-LIFT-181223/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of arbitrary CSV files on the server, which can contain sensitive information as well as removing those files from the server. **CVE ID : CVE-2023-6160**		
Vendor: Limesurvey					
Product: limesurvey					
Affected Version(s): * Up to (excluding) 6.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-2023	5.4	Cross Site Scripting (XSS) vulnerability in LimeSurvey before version 6.2.9-230925 allows a remote attacker to escalate privileges via a crafted script to the _generaloptions_panel.php component. **CVE ID : CVE-2023-44796**	https://github.com/LimeSurvey/LimeSurvey/pull/3483, https://github.com/limesurvey/limesurvey/commit/135511073c51c332613dd7fad9a8ca0aad34a3fe	A-LIM-LIME-181223/610
Vendor: limitloginattempts					
Product: limit_login_attempts_reloaded					
Affected Version(s): * Up to (excluding) 2.25.26					
Missing Authorization	27-Nov-2023	4.3	The Limit Login Attempts Reloaded WordPress plugin before 2.25.26 is missing authorization on the `toggle_auto_update` AJAX action, allowing any user with a valid nonce to toggle the auto-	N/A	A-LIM-LIMI-181223/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			update status of the plugin. **CVE ID : CVE-2023-5525**		
Vendor: Linecorp					
Product: line					
Affected Version(s): 13.6.1					
N/A	16-Nov-2023	7.5	nagayama_copabowl Line 13.6.1 is vulnerable to Exposure of Sensitive Information to an Unauthorized Actor. **CVE ID : CVE-2023-48134**	N/A	A-LIN-LINE-181223/612
Vendor: liquidweb					
Product: restrict_content					
Affected Version(s): * Up to (including) 3.2.7					
Exposure of Sensitive Information to an Unauthorized Actor	23-Nov-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in StellarWP Membership Plugin – Restrict Content plugin <= 3.2.7 versions. **CVE ID : CVE-2023-47668**	N/A	A-LIQ-REST-181223/613
Vendor: localstack					
Product: localstack					
Affected Version(s): 2.3.2					
Improper Certificate Validation	16-Nov-2023	7.4	Missing SSL certificate validation in localstack v2.3.2	N/A	A-LOC-LOCA-181223/614

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
			allows attackers to eavesdrop on communications between the host and server via a man-in-the-middle attack. **CVE ID : CVE-2023-48054**		
Vendor: luxsoft					
Product: luxcal_web_calendar					
Affected Version(s): * Up to (excluding) 5.2.4l					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Nov-2023	9.8	SQL injection vulnerability in LuxCal Web Calendar prior to 5.2.4M (MySQL version) and LuxCal Web Calendar prior to 5.2.4L (SQLite version) allows a remote unauthenticated attacker to execute an arbitrary SQL command by sending a crafted request, and obtain or alter information stored in the database. **CVE ID : CVE-2023-46700**	N/A	A-LUX-LUXC-181223/615
Improper Neutralization of Input During Web Page Generation	20-Nov-2023	6.1	Cross-site scripting vulnerability in LuxCal Web Calendar prior to 5.2.4M (MySQL version) and LuxCal Web Calendar prior to 5.2.4L (SQLite version) allows a	N/A	A-LUX-LUXC-181223/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			remote unauthenticated attacker to execute an arbitrary script on the web browser of the user who is accessing the product. **CVE ID : CVE-2023-47175**		
Affected Version(s): * Up to (excluding) 5.2.4m					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Nov-2023	9.8	SQL injection vulnerability in LuxCal Web Calendar prior to 5.2.4M (MySQL version) and LuxCal Web Calendar prior to 5.2.4L (SQLite version) allows a remote unauthenticated attacker to execute an arbitrary SQL command by sending a crafted request, and obtain or alter information stored in the database. **CVE ID : CVE-2023-46700**	N/A	A-LUX-LUXC-181223/617
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	6.1	Cross-site scripting vulnerability in LuxCal Web Calendar prior to 5.2.4M (MySQL version) and LuxCal Web Calendar prior to 5.2.4L (SQLite version) allows a remote	N/A	A-LUX-LUXC-181223/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to execute an arbitrary script on the web browser of the user who is accessing the product. **CVE ID : CVE-2023-47175**		
Vendor: lws					
Product: lws_tools					
Affected Version(s): * Up to (including) 2.3.1					
N/A	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in LWS LWS Tools plugin <= 2.3.1 versions. **CVE ID : CVE-2023-27453**	N/A	A-LWS-LWS_-181223/619
Vendor: m-files					
Product: m-files_server					
Affected Version(s): * Up to (excluding) 23.11.13156.0					
N/A	22-Nov-2023	5.3	Missing access permissions checks in the M-Files server before 23.11.13156.0 allow attackers to perform data write and export jobs using the M-Files API methods. **CVE ID : CVE-2023-6189**	N/A	A-M-F-M-FI-181223/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 23.11.13156.0					
N/A	22-Nov-2023	7.5	A possibility of unwanted server memory consumption was detected through the obsolete functionalities in the Rest API methods of the M-Files server before 23.11.13156.0 which allows attackers to execute DoS attacks. **CVE ID : CVE-2023-6117**	N/A	A-M-F-M-FI-181223/621
Vendor: m-privacy					
Product: mprivacy-tools					
Affected Version(s): * Up to (excluding) 2.0.406g					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-2023	6.5	In mprivacy-tools before 2.0.406g in m-privacy TightGate-Pro Server, a Directory Traversal in the print function of the VNC service allows authenticated attackers (with access to a VNC session) to automatically transfer malicious PDF documents by moving them into the .spool directory, and then sending a	N/A	A-M-P-MPRI-181223/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			signal to the VNC service, which automatically transfers them to the connected VNC client's filesystem. **CVE ID : CVE-2023-47251**		
Affected Version(s): * Up to (excluding) 4.0.406g					
Incorrect Default Permissions	22-Nov-2023	8.8	In mprivacy-tools before 2.0.406g in m-privacy TightGate-Pro Server, broken Access Control on X11 server sockets allows authenticated attackers (with access to a VNC session) to access the X11 desktops of other users by specifying their DISPLAY ID. This allows complete control of their desktop, including the ability to inject keystrokes and perform a keylogging attack. **CVE ID : CVE-2023-47250**	N/A	A-M-P-MPRI-181223/623
Product: rsbac-policy-tgpro					
Affected Version(s): * Up to (excluding) 2.0.159					
Incorrect Default Permissions	22-Nov-2023	8.8	In mprivacy-tools before 2.0.406g in m-privacy TightGate-Pro Server, broken Access Control on	N/A	A-M-P-RSBA-181223/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X11 server sockets allows authenticated attackers (with access to a VNC session) to access the X11 desktops of other users by specifying their DISPLAY ID. This allows complete control of their desktop, including the ability to inject keystrokes and perform a keylogging attack. **CVE ID : CVE-2023-47250**		
Product: tightgatevnc					
Affected Version(s): * Up to (excluding) 4.1.2-1					
Incorrect Default Permissions	22-Nov-2023	8.8	In mprivacy-tools before 2.0.406g in m-privacy TightGate-Pro Server, broken Access Control on X11 server sockets allows authenticated attackers (with access to a VNC session) to access the X11 desktops of other users by specifying their DISPLAY ID. This allows complete control of their desktop, including the ability to inject keystrokes and	N/A	A-M-P-TIGH-181223/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform a keylogging attack. **CVE ID : CVE-2023-47250**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-2023	6.5	In mprivacy-tools before 2.0.406g in m-privacy TightGate-Pro Server, a Directory Traversal in the print function of the VNC service allows authenticated attackers (with access to a VNC session) to automatically transfer malicious PDF documents by moving them into the .spool directory, and then sending a signal to the VNC service, which automatically transfers them to the connected VNC client's filesystem. **CVE ID : CVE-2023-47251**	N/A	A-M-P-TIGH-181223/626
Vendor: mage-people					
Product: bus_ticket_booking_with_seat_reservation					
Affected Version(s): * Up to (excluding) 5.2.6					
Improper Neutralization of Input During Web Page Generation	22-Nov-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MagePeople Team	N/A	A-MAG-BUS_-181223/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			WpBusTicketly plugin <= 5.2.5 versions. **CVE ID : CVE-2023-30496**		
Vendor: marcomilesi					
Product: anac_xml_bandi_di_gara					
Affected Version(s): * Up to (including) 7.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Marco Milesi ANAC XML Bandi di Gara plugin <= 7.5 versions. **CVE ID : CVE-2023-47242**	N/A	A-MAR-ANAC-181223/628
Product: anac_xml_viewer					
Affected Version(s): * Up to (including) 1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Marco Milesi ANAC XML Viewer plugin <= 1.7 versions. **CVE ID : CVE-2023-47245**	N/A	A-MAR-ANAC-181223/629
Vendor: mattermost					
Product: mattermost					
Affected Version(s): * Up to (including) 7.8.12					
Improper Neutralization of Special Elements in Output	27-Nov-2023	5.4	Mattermost fails to use innerText / textContent when setting the channel name in the webapp during	https://mattermost.com/security-updates	A-MAT-MATT-181223/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			autocomplete, allowing an attacker to inject HTML to a victim's page by create a channel name that is valid HTML. No XSS is possible though. **CVE ID : CVE-2023-35075**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.1.3					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-Nov-2023	5.4	Mattermost fails to use innerText / textContent when setting the channel name in the webapp during autocomplete, allowing an attacker to inject HTML to a victim's page by create a channel name that is valid HTML. No XSS is possible though. **CVE ID : CVE-2023-35075**	https://mattermost.com/security-updates	A-MAT-MATT-181223/631
Vendor: mayurik					
Product: best_courier_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input	27-Nov-2023	6.1	A vulnerability, which was classified as problematic, was	N/A	A-MAY-BEST-181223/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			found in SourceCodester Best Courier Management System 1.0. Affected is an unknown function. The manipulation of the argument page with the input </TiTlE><ScRiPt>alert(1)</ScRiPt> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-246126 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-6300**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Nov-2023	6.1	A vulnerability has been found in SourceCodester Best Courier Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file parcel_list.php of the component GET Parameter Handler. The manipulation of the	N/A	A-MAY-BEST-181223/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument id with the input </TiTlE><ScRiPt>alert(1)</ScRiPt> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-246127. **CVE ID : CVE-2023-6301**		
Vendor: mayuri_k					
Product: free_and_open_source_inventory_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Nov-2023	9.8	A vulnerability was found in SourceCodester Free and Open Source Inventory Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file ample/app/ajax/suppliar_data.php. The manipulation of the argument columns leads to sql injection. The attack may be initiated remotely.	https://vuldb.com/?ctiid.246131	A-MAY-FREE-181223/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-246131. **CVE ID : CVE-2023-6305**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Nov-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Free and Open Source Inventory Management System 1.0. Affected is an unknown function of the file /ample/app/ajax/member_data.php. The manipulation of the argument columns leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-246132. **CVE ID : CVE-2023-6306**	N/A	A-MAY-FREE-181223/635
Vendor: Mcafee					
Product: epolicy_orchestrator					
Affected Version(s): * Up to (excluding) 5.10.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Nov-2023	8	A Cross Site Request Forgery vulnerability in ePolicy Orchestrator prior to 5.10.0 CP1 Update 2 allows a remote low privilege user to successfully add a new user with administrator privileges to the ePO server. This impacts the dashboard area of the user interface. To exploit this the attacker must change the HTTP payload post submission, prior to it reaching the ePO server. **CVE ID : CVE-2023-5444**	N/A	A-MCA-EPOL-181223/636
N/A	17-Nov-2023	5.4	An open redirect vulnerability in ePolicy Orchestrator prior to 5.10.0 CP1 Update 2, allows a remote low privileged user to modify the URL parameter for the purpose of redirecting URL	https://kcm.trellix.com/corporate/index?page=content&id=SB10410	A-MCA-EPOL-181223/637

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
			request(s) to a malicious site. This impacts the dashboard area of the user interface. A user would need to be logged into ePO to trigger this vulnerability. To exploit this the attacker must change the HTTP payload post submission, prior to it reaching the ePO server. **CVE ID : CVE-2023-5445**		
Affected Version(s): 5.10.0					
N/A	17-Nov-2023	8	A Cross Site Request Forgery vulnerability in ePolicy Orchestrator prior to 5.10.0 CP1 Update 2 allows a remote low privilege user to successfully add a new user with administrator privileges to the ePO server. This impacts the dashboard area of the user interface. To exploit this the attacker must change the HTTP	N/A	A-MCA-EPOL-181223/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload post submission, prior to it reaching the ePO server. **CVE ID : CVE-2023-5444**		
N/A	17-Nov-2023	5.4	An open redirect vulnerability in ePolicy Orchestrator prior to 5.10.0 CP1 Update 2, allows a remote low privileged user to modify the URL parameter for the purpose of redirecting URL request(s) to a malicious site. This impacts the dashboard area of the user interface. A user would need to be logged into ePO to trigger this vulnerability. To exploit this the attacker must change the HTTP payload post submission, prior to it reaching the ePO server. **CVE ID : CVE-2023-5445**	https://kcm.trellix.com/corporate/index?page=content&id=SB10410	A-MCA-EPOL-181223/639

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: medart_notification_panel_project					
Product: medart_notification_panel					
Affected Version(s): * Up to (including) 2023-11-23					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Nov-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Medart Health Services Medart Notification Panel allows SQL Injection.This issue affects Medart Notification Panel: through 20231123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3631**	N/A	A-MED-MEDA-181223/640
Vendor: mediamanifesto					
Product: mmm_simple_file_list					
Affected Version(s): * Up to (including) 2.3					
Improper Neutralization of Input During	27-Nov-2023	5.4	The Mmm Simple File List WordPress plugin through 2.3 does not validate and escape some of	N/A	A-MED-MMM_-181223/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-4514**		
N/A	27-Nov-2023	4.3	The Mmm Simple File List WordPress plugin through 2.3 does not validate the generated path to list files from, allowing any authenticated users, such as subscribers, to list the content of arbitrary directories. **CVE ID : CVE-2023-4297**	N/A	A-MED-MMM_-181223/642
Vendor: mercedes-benz					
Product: mercedes_me					
Affected Version(s): * Up to (including) 1.34.0					
N/A	22-Nov-2023	5.3	An access control issue in Mercedes me IOS APP v1.34.0 and below allows attackers to view the carts of other users via sending a	N/A	A-MER-MERC-181223/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted add order request. **CVE ID : CVE-2023-47392**		
N/A	22-Nov-2023	5.3	An access control issue in Mercedes me IOS APP v1.34.0 and below allows attackers to view the maintenance orders of other users and access sensitive user information via unspecified vectors. **CVE ID : CVE-2023-47393**	N/A	A-MER-MERC-181223/644
Vendor: metagauss					
Product: eventprime					
Affected Version(s): * Up to (including) 3.2.9					
N/A	27-Nov-2023	5.3	The EventPrime WordPress plugin through 3.2.9 specifies the price of a booking in the client request, allowing an attacker to purchase bookings without payment. **CVE ID : CVE-2023-4252**	N/A	A-MET-EVEN-181223/645
Product: profilegrid					
Affected Version(s): * Up to (including) 5.6.6					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in profilegrid ProfileGrid – User Profiles,	N/A	A-MET-PROF-181223/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Memberships, Groups and Communities.This issue affects ProfileGrid – User Profiles, Memberships, Groups and Communities: from n/a through 5.6.6. **CVE ID : CVE-2023-47644**		
Vendor: Microsoft					
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 119.0.2151.72					
N/A	16-Nov-2023	6.6	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability **CVE ID : CVE-2023-36008**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36008	A-MIC-EDGE-181223/647
N/A	16-Nov-2023	4.3	Microsoft Edge (Chromium-based) Spoofing Vulnerability **CVE ID : CVE-2023-36026**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36026	A-MIC-EDGE-181223/648
Vendor: mingocommerce					
Product: woocommerce_product_enquiry					
Affected Version(s): * Up to (including) 2.3.4					
Improper Neutralization of Input During Web Page	16-Nov-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in MingoCommerce WooCommerce Product Enquiry	N/A	A-MIN-WOOC-181223/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			plugin <= 2.3.4 versions. **CVE ID : CVE-2023-32796**		
Vendor: Misp-project					
Product: malware_information_sharing_platform					
Affected Version(s): * Up to (excluding) 2.4.176					
N/A	17-Nov-2023	9.8	An issue was discovered in MISP before 2.4.176. app/Controller/Component/IndexFilterComponent.php does not properly filter out query parameters. **CVE ID : CVE-2023-48655**	https://github.com/MISP/MISP/compare/v2.4.175...v2.4.176 , https://github.com/MISP/MISP/commit/158c8b2f788b75e0d26e9249a75e1be291e59d4b	A-MIS-MALW-181223/650
N/A	17-Nov-2023	9.8	An issue was discovered in MISP before 2.4.176. app/Model/AppModel.php mishandles order clauses. **CVE ID : CVE-2023-48656**	https://github.com/MISP/MISP/compare/v2.4.175...v2.4.176 , https://github.com/MISP/MISP/commit/d6ad402b31547c95280a6d8320f8f87a8f609074	A-MIS-MALW-181223/651
N/A	17-Nov-2023	9.8	An issue was discovered in MISP before 2.4.176. app/Model/AppModel.php mishandles filters. **CVE ID : CVE-2023-48657**	https://github.com/MISP/MISP/compare/v2.4.175...v2.4.176 , https://github.com/MISP/MISP/commit/08bd23281ead288de678de666ef43ed6de1899fc	A-MIS-MALW-181223/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Nov-2023	9.8	An issue was discovered in MISP before 2.4.176. app/Model/AppModel.php lacks a checkParam function for alphanumerics, underscore, dash, period, and space. **CVE ID : CVE-2023-48658**	https://github.com/MISP/MISP/compare/v2.4.175...v2.4.176 , https://github.com/MISP/MISP/commit/168621521b57b2437331174186f84a6aa3e71f0d	A-MIS-MALW-181223/653
N/A	17-Nov-2023	9.8	An issue was discovered in MISP before 2.4.176. app/Controller/AppController.php mishandles parameter parsing. **CVE ID : CVE-2023-48659**	https://github.com/MISP/MISP/compare/v2.4.175...v2.4.176 , https://github.com/MISP/MISP/commit/37ecf81b84a01baa4d4b1fade4de94a9018c32ed	A-MIS-MALW-181223/654
Vendor: mizhexiaoxiao					
Product: websiteguide					
Affected Version(s): 0.2					
N/A	20-Nov-2023	9.8	An Insecure Permissions issue in WebsiteGuide v.0.2 allows a remote attacker to gain escalated privileges via crafted jwt (JSON web token). **CVE ID : CVE-2023-48176**	N/A	A-MIZ-WEBS-181223/655
Vendor: mmrs151					
Product: daily_prayer_time					
Affected Version(s): * Up to (including) 2023.10.13					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mmrs151 Daily Prayer Time plugin <= 2023.10.13 versions. **CVE ID : CVE-2023-47817**	N/A	A-MMR-DAIL-181223/656
Vendor: mondula					
Product: multi_step_form					
Affected Version(s): * Up to (excluding) 1.7.11					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Mondula GmbH Multi Step Form plugin <= 1.7.11 versions. **CVE ID : CVE-2023-47758**	N/A	A-MON-MULT-181223/657
Vendor: moses-smt					
Product: mosesdecoder					
Affected Version(s): * Up to (excluding) 4.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Nov-2023	9.8	A vulnerability, which was classified as critical, was found in moses-smt mosesdecoder up to 4.0. This affects an unknown part of the file contrib/iSenWeb/trans_result.php. The manipulation of the argument	N/A	A-MOS-MOSE-181223/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input1 leads to os command injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-246135. **CVE ID : CVE-2023-6309**		
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 120.0					
N/A	21-Nov-2023	9.8	An attacker could have accessed internal pages or data by ex-filtrating a security key from ReaderMode via the `referrerpolicy` attribute. This vulnerability affects Firefox for iOS < 120. **CVE ID : CVE-2023-49060**	https://www.mozilla.org/security/advisories/mfsa2023-51/	A-MOZ-FIRE-181223/659
Use After Free	21-Nov-2023	8.8	Ownership mismanagement led to a use-after-free in ReadableByteStreams This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5.	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisorie	A-MOZ-FIRE-181223/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6207	s/mfsa2023-52/	
N/A	21-Nov-2023	8.8	When using X11, text selected by the page using the Selection API was erroneously copied into the primary selection, a temporary storage not unlike the clipboard. *This bug only affects Firefox on X11. Other systems are unaffected.* This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6208**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-FIRE-181223/661
Out-of-bounds Write	21-Nov-2023	8.8	Memory safety bugs present in Firefox 119, Firefox ESR 115.4, and Thunderbird 115.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-FIRE-181223/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.5. **CVE ID : CVE-2023-6212**		
Out-of-bounds Write	21-Nov-2023	8.8	Memory safety bugs present in Firefox 119. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 120. **CVE ID : CVE-2023-6213**	https://www.mozilla.org/security/advisories/mfsa2023-49/	A-MOZ-FIRE-181223/663
Out-of-bounds Read	21-Nov-2023	6.5	On some systems—depending on the graphics settings and drivers—it was possible to force an out-of-bounds read and leak memory data into the images created on the canvas element. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6204**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-FIRE-181223/664
Use After Free	21-Nov-2023	6.5	It was possible to cause the use of a MessagePort after it had already been	https://www.mozilla.org/security/advisories/mfsa2023-	A-MOZ-FIRE-181223/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			freed, which could potentially have led to an exploitable crash. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6205**	49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	6.5	Relative URLs starting with three slashes were incorrectly parsed, and a path-traversal "/../" part in the path could be used to override the specified host. This could contribute to security problems in web sites. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6209**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-FIRE-181223/666
N/A	21-Nov-2023	6.5	When an https: web page created a pop-up from a "javascript:" URL, that pop-up was incorrectly allowed to load blockable content such as iframes from insecure http: URLs	https://www.mozilla.org/security/advisories/mfsa2023-49/	A-MOZ-FIRE-181223/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability affects Firefox < 120. **CVE ID : CVE-2023-6210**		
Improper Restriction of Rendered UI Layers or Frames	21-Nov-2023	6.5	If an attacker needed a user to load an insecure http: page and knew that user had enabled HTTPS-only mode, the attacker could have tricked the user into clicking to grant an HTTPS-only exception if they could get the user to participate in a clicking game. This vulnerability affects Firefox < 120. **CVE ID : CVE-2023-6211**	https://www.mozilla.org/security/advisories/mfsa2023-49/	A-MOZ-FIRE-181223/668
URL Redirection to Untrusted Site ('Open Redirect')	21-Nov-2023	6.1	An attacker could have performed HTML template injection via Reader Mode and exfiltrated user information. This vulnerability affects Firefox for iOS < 120. **CVE ID : CVE-2023-49061**	https://www.mozilla.org/security/advisories/mfsa2023-51/	A-MOZ-FIRE-181223/669
Improper Restriction of Rendered	21-Nov-2023	5.4	The black fade animation when exiting fullscreen is roughly the length of the anti-	https://www.mozilla.org/security/advisories/mfsa2023-49/,	A-MOZ-FIRE-181223/670

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
UI Layers or Frames			clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6206**	https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	
Product: firefox_esr					
Affected Version(s): * Up to (excluding) 115.5.0					
Use After Free	21-Nov-2023	8.8	Ownership mismanagement led to a use-after-free in ReadableByteStreams This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6207**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-FIRE-181223/671
N/A	21-Nov-2023	8.8	When using X11, text selected by the page using the Selection API was erroneously copied into the primary selection, a	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/sec	A-MOZ-FIRE-181223/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			temporary storage not unlike the clipboard. *This bug only affects Firefox on X11. Other systems are unaffected.* This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6208**	urity/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	
Out-of-bounds Write	21-Nov-2023	8.8	Memory safety bugs present in Firefox 119, Firefox ESR 115.4, and Thunderbird 115.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6212**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-FIRE-181223/673
Out-of-bounds Read	21-Nov-2023	6.5	On some systems—depending on the graphics settings and drivers—it was possible to force an	https://www.mozilla.org/security/advisories/mfsa2023-49/,	A-MOZ-FIRE-181223/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out-of-bounds read and leak memory data into the images created on the canvas element. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6204**	https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	
Use After Free	21-Nov-2023	6.5	It was possible to cause the use of a MessagePort after it had already been freed, which could potentially have led to an exploitable crash. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6205**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-FIRE-181223/675
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	6.5	Relative URLs starting with three slashes were incorrectly parsed, and a path-traversal "/../" part in the path could be used to override the specified host. This could contribute to security problems in web sites. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisorie	A-MOZ-FIRE-181223/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6209**	s/mfsa2023-52/	
Improper Restriction of Rendered UI Layers or Frames	21-Nov-2023	5.4	The black fade animation when exiting fullscreen is roughly the length of the anti-clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6206**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-FIRE-181223/677
Product: thunderbird					
Affected Version(s): * Up to (excluding) 115.5					
Use After Free	21-Nov-2023	8.8	Ownership mismanagement led to a use-after-free in ReadableByteStreams This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/,	A-MOZ-THUN-181223/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.5. **CVE ID : CVE-2023-6207**	https://www.mozilla.org/security/advisories/mfsa2023-52/	
N/A	21-Nov-2023	8.8	When using X11, text selected by the page using the Selection API was erroneously copied into the primary selection, a temporary storage not unlike the clipboard. *This bug only affects Firefox on X11. Other systems are unaffected.* This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6208**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-THUN-181223/679
Out-of-bounds Write	21-Nov-2023	8.8	Memory safety bugs present in Firefox 119, Firefox ESR 115.4, and Thunderbird 115.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 120,	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-THUN-181223/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6212**		
Out-of-bounds Read	21-Nov-2023	6.5	On some systems—depending on the graphics settings and drivers—it was possible to force an out-of-bounds read and leak memory data into the images created on the canvas element. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6204**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-THUN-181223/681
Use After Free	21-Nov-2023	6.5	It was possible to cause the use of a MessagePort after it had already been freed, which could potentially have led to an exploitable crash. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6205**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-THUN-181223/682
Improper Limitation	21-Nov-2023	6.5	Relative URLs starting with three	https://www.mozilla.org/sec	A-MOZ-THUN-181223/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			slashes were incorrectly parsed, and a path-traversal "/../" part in the path could be used to override the specified host. This could contribute to security problems in web sites. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6209**	urity/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	
Improper Restriction of Rendered UI Layers or Frames	21-Nov-2023	5.4	The black fade animation when exiting fullscreen is roughly the length of the anti-clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6206**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	A-MOZ-THUN-181223/684

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: myaudiomerchant					
Product: audio_merchant					
Affected Version(s): * Up to (including) 5.0.4					
Cross-Site Request Forgery (CSRF)	20-Nov-2023	8.8	The Audio Merchant plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.0.4. This is due to missing or incorrect nonce validation on the function audio_merchant_add_audio_file function. This makes it possible for unauthenticated attackers to upload arbitrary files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-6196**	N/A	A-MYA-AUDI-181223/685
Cross-Site Request Forgery (CSRF)	20-Nov-2023	5.4	The Audio Merchant plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.0.4. This is due to missing or	N/A	A-MYA-AUDI-181223/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incorrect nonce validation on the audio_merchant_save_settings function. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-6197**		
Vendor: myprestamodules					
Product: cross_selling_in_modal_cart					
Affected Version(s): * Up to (excluding) 3.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Nov-2023	9.8	In the module "Cross Selling in Modal Cart" (motivationsale) < 3.5.0 from MyPrestaModules for PrestaShop, a guest can perform SQL injection. The method `motivationsaleDataModel::getProductsByIds()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	https://security.friendsofpresta.org/modules/2023/11/21/motivationsale.html	A-MYP-CROS-181223/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46357		
Product: exportproducts					
Affected Version(s): * Up to (excluding) 5.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Nov-2023	9.8	In the module "Product Catalog (CSV, Excel, XML) Export PRO" (exportproducts) in versions up to 5.0.0 from MyPrestaModules for PrestaShop, a guest can perform SQL injection via `exportProduct::_addDataToDb().` **CVE ID : CVE-2023-45387**	https://security.friendsofpresta.org/modules/2023/11/16/exportproducts.html	A-MYP-EXPO-181223/688
Vendor: nautobot					
Product: nautobot-plugin-device-onboarding					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 3.0.0					
N/A	21-Nov-2023	6.5	The Nautobot Device Onboarding plugin uses the netmiko and NAPALM libraries to simplify the onboarding process of a new device into Nautobot down to, in many cases, an IP Address and a Location. Starting in version 2.0.0 and prior to version 3.0.0, credentials provided to onboarding task are visible via Job Results from an	https://github.com/nautobot/nautobot-plugin-device-onboarding/security/advisories/GHSA-qf3c-rw9f-jh7v	A-NAU-NAUT-181223/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution of an Onboarding Task. Version 3.0.0 fixes this issue; no known workarounds are available. Mitigation recommendations include deleting all Job Results for any onboarding task to remove clear text credentials from database entries that were run while on v2.0.X, upgrading to v3.0.0, and rotating any exposed credentials. **CVE ID : CVE-2023-48700**		
Vendor: nayemhowlader					
Product: sup_online_shopping					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	Cross Site Scripting in SUP Online Shopping v.1.0 allows a remote attacker to execute arbitrary code via the Name, Email and Address parameters in the Register New Account component. **CVE ID : CVE-2023-48124**	N/A	A-NAY-SUP_-181223/690
Vendor: nc3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: testing_platform					
Affected Version(s): * Up to (excluding) 2.1.1					
N/A	20-Nov-2023	7.5	TestingPlatform is a testing platform for Internet Security Standards. Prior to version 2.1.1, user input is not filtered correctly. Nmap options are accepted. In this particular case, the option to create log files is accepted in addition to a host name (and even without). A log file is created at the location specified. These files are created as root. If the file exists, the existing file is being rendered useless. This can result in denial of service. Additionally, input for scanning can be any CIDR blocks passed to nmap. An attacker can scan 0.0.0.0/0 or even local networks. Version 2.1.1 contains a patch for this issue. **CVE ID : CVE-2023-48310**	https://github.com/NC3-LU/TestingPlatform/commit/7b3e7ca869a4845aa7445f874c22c5929315c3a7, https://github.com/NC3-LU/TestingPlatform/security/advisories/GHSA-mmpf-rw6c-67mm	A-NC3-TEST-181223/691
Vendor: nearform					
Product: fast-jwt					
Affected Version(s): * Up to (excluding) 3.3.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Nov-2023	5.9	fast-jwt provides fast JSON Web Token (JWT) implementation. Prior to version 3.3.2, the fast-jwt library does not properly prevent JWT algorithm confusion for all public key types. The 'publicKeyPemMatcher' in 'fast-jwt/src/crypto.js' does not properly match all common PEM formats for public keys. To exploit this vulnerability, an attacker needs to craft a malicious JWT token containing the HS256 algorithm, signed with the public RSA key of the victim application. This attack will only work if the victim application utilizes a public key containing the `BEGIN RSA PUBLIC KEY` header. Applications using the RS256 algorithm, a public key with a `BEGIN RSA PUBLIC KEY` header, and calling the verify function	https://github.com/nearform/fast-jwt/security/advisories/GHSA-c2ff-88x2-x9pg	A-NEA-FAST-181223/692

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
			without explicitly providing an algorithm, are vulnerable to this algorithm confusion attack which allows attackers to sign arbitrary payloads which will be accepted by the verifier. Version 3.3.2 contains a patch for this issue. As a workaround, change line 29 of `blob/master/src/crypto.js` to include a regular expression. **CVE ID : CVE-2023-48223**		
Vendor: NEC					
Product: expresscluster_x					
Affected Version(s): 1.0					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/694
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/696
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 3.1					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/698
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/700
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/702
Affected Version(s): 3.2					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/703

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-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/704
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/706
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 2.0					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/708
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/710
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/712
Affected Version(s): 2.1					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/714
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/716
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 3.0					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/718
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/720
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/722
Affected Version(s): 3.3					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/724
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/726
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 4.0					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/728
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/730
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/732
Affected Version(s): 4.1					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/734
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/736
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 4.2					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/738
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/740
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/742
Affected Version(s): 4.3					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/744
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/746
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 5.0					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/748
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/750
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/752
Affected Version(s): 5.1					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/754
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Product: expresscluster_x_singleserversafe					
Affected Version(s): 1.0					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/756
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/757

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-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/758
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/760
Affected Version(s): 3.1					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/762
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/764
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 3.2					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/766
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/767

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-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/768
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/770
Affected Version(s): 2.0					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/772
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/774
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 2.1					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/776
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/778
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/780
Affected Version(s): 3.0					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/782
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/784
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 3.3					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/786
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/788
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/790
Affected Version(s): 4.0					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/792
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/794
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 4.1					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/796
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/798
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/799

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-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/800
Affected Version(s): 4.2					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/802
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/804
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 4.3					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/806
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/808
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39547		
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39548**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/810
Affected Version(s): 5.0					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39544		
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39545**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/812
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	N/A	A-NEC-EXPR-181223/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39546		
Authentication Bypass by Capture-replay	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39547**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/814
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39548		
Affected Version(s): 5.1					
Missing Authorization	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39544**	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/816
Files or Directories Accessible to External Parties	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command.	https://jpn.nec.com/security-info/secinfo/nv23-009_en.html	A-NEC-EXPR-181223/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39545		
N/A	17-Nov-2023	8.8	CLUSTERPRO X Ver5.1 and earlier and EXPRESSCLUSTER X 5.1 and earlier, CLUSTERPRO X SingleServerSafe 5.1 and earlier, EXPRESSCLUSTER X SingleServerSafe 5.1 and earlier allows a attacker to log in to the product may execute an arbitrary command. **CVE ID : CVE-2023-39546**	N/A	A-NEC-EXPR-181223/818
Vendor: networktocode					
Product: nautobot					
Affected Version(s): * Up to (excluding) 1.6.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Nautobot is a Network Source of Truth and Network Automation Platform built as a web application All users of Nautobot versions earlier than 1.6.6 or 2.0.5 are potentially affected by a cross-site scripting vulnerability. Due to incorrect usage of Django's `mark_safe()` API	https://github.com/nautobot/nautobot/security/advisories/GHSA-cf9f-wmhp-v4pr, https://github.com/nautobot/nautobot/pull/4832, https://github.com/nautobot/nautobot/pull/4833	A-NET-NAUT-181223/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when rendering certain types of user-authored content; including custom links, job buttons, and computed fields; it is possible that users with permission to create or edit these types of content could craft a malicious payload (such as JavaScript code) that would be executed when rendering pages containing this content. The maintainers have fixed the incorrect uses of `mark_safe()` (generally by replacing them with appropriate use of `format_html()` instead) to prevent such malicious data from being executed. Users on Nautobot 1.6.x LTM should upgrade to v1.6.6 and users on Nautobot 2.0.x should upgrade to v2.0.5. Appropriate object permissions can and should be applied to restrict which users are permitted to create		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or edit the aforementioned types of user-authored content. Other than that, there is no direct workaround available. **CVE ID : CVE-2023-48705**		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Nautobot is a Network Source of Truth and Network Automation Platform built as a web application All users of Nautobot versions earlier than 1.6.6 or 2.0.5 are potentially affected by a cross-site scripting vulnerability. Due to incorrect usage of Django's `mark_safe()` API when rendering certain types of user-authored content; including custom links, job buttons, and computed fields; it is possible that users with permission to create or edit these types of content could craft a malicious payload (such as JavaScript code) that would be	https://github.com/nautobot/nautobot/security/advisories/GHSA-cf9f-wmhp-v4pr, https://github.com/nautobot/nautobot/pull/4832, https://github.com/nautobot/nautobot/pull/4833	A-NET-NAUT-181223/820

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
			executed when rendering pages containing this content. The maintainers have fixed the incorrect uses of `mark_safe()` (generally by replacing them with appropriate use of `format_html()` instead) to prevent such malicious data from being executed. Users on Nautobot 1.6.x LTM should upgrade to v1.6.6 and users on Nautobot 2.0.x should upgrade to v2.0.5. Appropriate object permissions can and should be applied to restrict which users are permitted to create or edit the aforementioned types of user-authored content. Other than that, there is no direct workaround available. **CVE ID : CVE-2023-48705**		
Vendor: nextauth.js					
Product: next-auth					
Affected Version(s): * Up to (excluding) 4.24.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	20-Nov-2023	5.3	NextAuth.js provides authentication for Next.js. `next-auth` applications prior to version 4.24.5 that rely on the default Middleware authorization are affected by a vulnerability. A bad actor could create an empty/mock user, by getting hold of a NextAuth.js-issued JWT from an interrupted OAuth sign-in flow (state, PKCE or nonce). Manually overriding the `next-auth.session-token` cookie value with this non-related JWT would let the user simulate a logged in user, albeit having no user information associated with it. (The only property on this user is an opaque randomly generated string). This vulnerability does not give access to other users' data, neither to resources that require proper authorization via scopes or other means. The created	https://github.com/nextauthjs/next-auth/security/advisories/GHSA-v64w-49xw-qq89, https://github.com/nextauthjs/next-auth/commit/d237059b6d0cb868c041ba18b698e0cee20a2f10	A-NEX-NEXT-181223/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mock user has no information associated with it (ie. no name, email, access_token, etc.) This vulnerability can be exploited by bad actors to peek at logged in user states (e.g. dashboard layout). `next-auth` `v4.24.5` contains a patch for the vulnerability. As a workaround, using a custom authorization callback for Middleware, developers can manually do a basic authentication. **CVE ID : CVE-2023-48309**		
Vendor: Nextcloud					
Product: mail					
Affected Version(s): From (including) 1.13.0 Up to (excluding) 2.2.8					
N/A	21-Nov-2023	9.8	Nextcloud Mail is the mail app for Nextcloud, a self-hosted productivity platform. Starting in version 1.13.0 and prior to version 2.2.8 and 3.3.0, an attacker can use an unprotected endpoint in the Mail app to perform a SSRF attack. Nextcloud Mail app	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-4pp4-m8ph-2999, https://github.com/nextcloud/mail/pull/8709	A-NEX-MAIL-181223/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 2.2.8 and 3.3.0 contain a patch for this issue. As a workaround, disable the mail app. **CVE ID : CVE-2023-48307**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.3.0					
N/A	21-Nov-2023	9.8	Nextcloud Mail is the mail app for Nextcloud, a self-hosted productivity platform. Starting in version 1.13.0 and prior to version 2.2.8 and 3.3.0, an attacker can use an unprotected endpoint in the Mail app to perform a SSRF attack. Nextcloud Mail app versions 2.2.8 and 3.3.0 contain a patch for this issue. As a workaround, disable the mail app. **CVE ID : CVE-2023-48307**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-4pp4-m8ph-2999, https://github.com/nextcloud/mail/pull/8709	A-NEX-MAIL-181223/823
Product: nextcloud_server					
Affected Version(s): From (including) 20.0.0 Up to (excluding) 20.0.14.16					
N/A	21-Nov-2023	7.1	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13,	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-f962-hw26-g267, https://github.com/nextcloud	A-NEX-NEXT-181223/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	26.0.8, and 27.1.3 of Nextcloud Server and starting in version 20.0.0 and prior to versions 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Enterprise Server, a malicious user could update any personal or global external storage, making them inaccessible for everyone else as well. Nextcloud Server 25.0.13, 26.0.8, and 27.1.3 and Nextcloud Enterprise Server is upgraded to 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 contain a patch for this issue. As a workaround, disable app files_external. This workaround also makes the external storage inaccessible but retains the configurations until a patched version has been deployed.	/server/pull/41123	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48239		
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.0.9.13					
N/A	21-Nov-2023	7.1	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and starting in version 20.0.0 and prior to versions 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Enterprise Server, a malicious user could update any personal or global external storage, making them inaccessible for everyone else as well. Nextcloud Server 25.0.13, 26.0.8, and 27.1.3 and Nextcloud Enterprise Server is upgraded to 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13,	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-f962-hw26-g267, https://github.com/nextcloud/server/pull/41123	A-NEX-NEXT-181223/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			26.0.8, and 27.1.3 contain a patch for this issue. As a workaround, disable app files_external. This workaround also makes the external storage inaccessible but retains the configurations until a patched version has been deployed. **CVE ID : CVE-2023-48239**		
Affected Version(s): From (including) 22.0.0 Up to (excluding) 22.2.10.15					
N/A	21-Nov-2023	7.1	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and starting in version 20.0.0 and prior to versions 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Enterprise Server, a malicious user could update any personal or global external storage, making them	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-f962-hw26-g267, https://github.com/nextcloud/server/pull/41123	A-NEX-NEXT-181223/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inaccessible for everyone else as well. Nextcloud Server 25.0.13, 26.0.8, and 27.1.3 and Nextcloud Enterprise Server is upgraded to 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 contain a patch for this issue. As a workaround, disable app files_external. This workaround also makes the external storage inaccessible but retains the configurations until a patched version has been deployed. **CVE ID : CVE-2023-48239**		
Affected Version(s): From (including) 22.0.0 Up to (excluding) 22.2.10.16					
Server-Side Request Forgery (SSRF)	21-Nov-2023	9.8	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and starting in version 22.0.0 and prior to versions	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8f69-f9jg-4x3v, https://github.com/nextcloud/server/pull/40234	A-NEX-NEXT-181223/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Enterprise Server, the DNS pin middleware was vulnerable to DNS rebinding allowing an attacker to perform SSRF as a final result. Nextcloud Server 25.0.11, 26.0.6, and 27.1.0 and Nextcloud Enterprise Server 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 contain patches for this issue. No known workarounds are available. **CVE ID : CVE-2023-48306**		
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.12.11					
Server-Side Request Forgery (SSRF)	21-Nov-2023	9.8	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and starting in version 22.0.0 and	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8f69-f9jg-4x3v, https://github.com/nextcloud/server/pull/40234	A-NEX-NEXT-181223/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to versions 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Enterprise Server, the DNS pin middleware was vulnerable to DNS rebinding allowing an attacker to perform SSRF as a final result. Nextcloud Server 25.0.11, 26.0.6, and 27.1.0 and Nextcloud Enterprise Server 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 contain patches for this issue. No known workarounds are available. **CVE ID : CVE-2023-48306**		
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.12.12					
N/A	21-Nov-2023	7.1	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and starting in	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-f962-hw26-g267, https://github.com/nextcloud/server/pull/41123	A-NEX-NEXT-181223/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 20.0.0 and prior to versions 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Enterprise Server, a malicious user could update any personal or global external storage, making them inaccessible for everyone else as well. Nextcloud Server 25.0.13, 26.0.8, and 27.1.3 and Nextcloud Enterprise Server is upgraded to 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 contain a patch for this issue. As a workaround, disable app files_external. This workaround also makes the external storage inaccessible but retains the configurations until a patched version has been deployed. **CVE ID : CVE-2023-48239**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.12.7					
Server-Side Request Forgery (SSRF)	21-Nov-2023	9.8	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and starting in version 22.0.0 and prior to versions 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Enterprise Server, the DNS pin middleware was vulnerable to DNS rebinding allowing an attacker to perform SSRF as a final result. Nextcloud Server 25.0.11, 26.0.6, and 27.1.0 and Nextcloud Enterprise Server 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 contain patches for this issue. No known workarounds are available.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8f69-f9jg-4x3v, https://github.com/nextcloud/server/pull/40234	A-NEX-NEXT-181223/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	**CVE ID : CVE-2023-48306**		
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.12.8					
N/A	21-Nov-2023	7.1	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and starting in version 20.0.0 and prior to versions 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Enterprise Server, a malicious user could update any personal or global external storage, making them inaccessible for everyone else as well. Nextcloud Server 25.0.13, 26.0.8, and 27.1.3 and Nextcloud Enterprise Server is upgraded to 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13,	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-f962-hw26-g267, https://github.com/nextcloud/server/pull/41123	A-NEX-NEXT-181223/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			26.0.8, and 27.1.3 contain a patch for this issue. As a workaround, disable app files_external. This workaround also makes the external storage inaccessible but retains the configurations until a patched version has been deployed. **CVE ID : CVE-2023-48239**		
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.11					
Server-Side Request Forgery (SSRF)	21-Nov-2023	9.8	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and starting in version 22.0.0 and prior to versions 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Enterprise Server, the DNS pin middleware was vulnerable to DNS rebinding allowing an attacker to perform SSRF as a final result.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8f69-f9jg-4x3v, https://github.com/nextcloud/server/pull/40234	A-NEX-NEXT-181223/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Nextcloud Server 25.0.11, 26.0.6, and 27.1.0 and Nextcloud Enterprise Server 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 contain patches for this issue. No known workarounds are available. **CVE ID : CVE-2023-48306**		
N/A	21-Nov-2023	4.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and Nextcloud Enterprise Server, when the log level was set to debug, the user_ldap app logged user passwords in plaintext into the log file. If the log file was then leaked or shared in any way the users' passwords would be leaked. Nextcloud Server and Nextcloud	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-35p6-4992-w5fr, https://github.com/nextcloud/server/pull/40013	A-NEX-NEXT-181223/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Server versions 25.0.11, 26.0.6, and 27.1.0 contain a patch for this issue. As a workaround, change config setting \`loglevel\` to \`1\` or higher (should always be higher than 1 in production environments). **CVE ID : CVE-2023-48305**		
N/A	21-Nov-2023	2.7	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and Nextcloud Enterprise Server, admins can change authentication details of user configured external storage. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.11, 26.0.6, and 27.1.0 contain a patch for this issue. No known workarounds are available.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-2448-44rp-c7hh, https://github.com/nextcloud/server/pull/39895	A-NEX-NEXT-181223/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48303		
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.13					
N/A	21-Nov-2023	7.1	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and starting in version 20.0.0 and prior to versions 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Enterprise Server, a malicious user could update any personal or global external storage, making them inaccessible for everyone else as well. Nextcloud Server 25.0.13, 26.0.8, and 27.1.3 and Nextcloud Enterprise Server is upgraded to 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13,	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-f962-hw26-g267, https://github.com/nextcloud/server/pull/41123	A-NEX-NEXT-181223/835

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
			26.0.8, and 27.1.3 contain a patch for this issue. As a workaround, disable app files_external. This workaround also makes the external storage inaccessible but retains the configurations until a patched version has been deployed. **CVE ID : CVE-2023-48239**		
N/A	21-Nov-2023	5.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and Nextcloud Enterprise Server, an attacker could insert links into circles name that would be opened when clicking the circle name in a search filter. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.13, 26.0.8, and 27.1.3 contain a fix for this issue. As a	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-wgpw-qqq2-gwv6, https://github.com/nextcloud/circles/pull/1415	A-NEX-NEXT-181223/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workaround, disable app circles. **CVE ID : CVE-2023-48301**		
N/A	21-Nov-2023	5.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and Nextcloud Enterprise Server, when a user is tricked into copy pasting HTML code without markup (Ctrl+Shift+V) the markup will actually render. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.13, 26.0.8, and 27.1.3 contain a fix for this issue. As a workaround, disable app text. **CVE ID : CVE-2023-48302**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-p7g9-x25m-4h87, https://github.com/nextcloud/text/pull/4877	A-NEX-NEXT-181223/837
Affected Version(s): From (including) 25.0.0 Up to (including) 25.0.13					
N/A	21-Nov-2023	5.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-wgpw-	A-NEX-NEXT-181223/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and Nextcloud Enterprise Server, an attacker could insert links into circles name that would be opened when clicking the circle name in a search filter. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.13, 26.0.8, and 27.1.3 contain a fix for this issue. As a workaround, disable app circles. **CVE ID : CVE-2023-48301**	qqq2-gwv6, https://github.com/nextcloud/circles/pull/1415	
Affected Version(s): From (including) 26.0.0 Up to (excluding) 26.0.6					
Server-Side Request Forgery (SSRF)	21-Nov-2023	9.8	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and starting in version 22.0.0 and prior to versions 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11,	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8f69-f9jg-4x3v, https://github.com/nextcloud/server/pull/40234	A-NEX-NEXT-181223/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			26.0.6, and 27.1.0 of Nextcloud Enterprise Server, the DNS pin middleware was vulnerable to DNS rebinding allowing an attacker to perform SSRF as a final result. Nextcloud Server 25.0.11, 26.0.6, and 27.1.0 and Nextcloud Enterprise Server 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 contain patches for this issue. No known workarounds are available. **CVE ID : CVE-2023-48306**		
N/A	21-Nov-2023	4.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and Nextcloud Enterprise Server, when the log level was set to debug, the user_ldap app logged user	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-35p6-4992-w5fr, https://github.com/nextcloud/server/pull/40013	A-NEX-NEXT-181223/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passwords in plaintext into the log file. If the log file was then leaked or shared in any way the users' passwords would be leaked. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.11, 26.0.6, and 27.1.0 contain a patch for this issue. As a workaround, change config setting `loglevel` to `1` or higher (should always be higher than 1 in production environments). **CVE ID : CVE-2023-48305**		
N/A	21-Nov-2023	2.7	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and Nextcloud Enterprise Server, admins can change authentication details of user configured external storage. Nextcloud	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-2448-44rp-c7hh, https://github.com/nextcloud/server/pull/39895	A-NEX-NEXT-181223/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server and Nextcloud Enterprise Server versions 25.0.11, 26.0.6, and 27.1.0 contain a patch for this issue. No known workarounds are available. **CVE ID : CVE-2023-48303**		
Affected Version(s): From (including) 26.0.0 Up to (excluding) 26.0.8					
N/A	21-Nov-2023	7.1	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and starting in version 20.0.0 and prior to versions 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Enterprise Server, a malicious user could update any personal or global external storage, making them inaccessible for everyone else as well. Nextcloud	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-f962-hw26-g267, https://github.com/nextcloud/server/pull/41123	A-NEX-NEXT-181223/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server 25.0.13, 26.0.8, and 27.1.3 and Nextcloud Enterprise Server is upgraded to 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 contain a patch for this issue. As a workaround, disable app files_external. This workaround also makes the external storage inaccessible but retains the configurations until a patched version has been deployed. **CVE ID : CVE-2023-48239**		
N/A	21-Nov-2023	5.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and Nextcloud Enterprise Server, an attacker could insert links into circles name that would be opened when clicking the	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-wgpw-qqq2-gwv6, https://github.com/nextcloud/circles/pull/1415	A-NEX-NEXT-181223/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			circle name in a search filter. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.13, 26.0.8, and 27.1.3 contain a fix for this issue. As a workaround, disable app circles. **CVE ID : CVE-2023-48301**		
N/A	21-Nov-2023	5.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and Nextcloud Enterprise Server, when a user is tricked into copy pasting HTML code without markup (Ctrl+Shift+V) the markup will actually render. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.13, 26.0.8, and 27.1.3 contain a fix for this issue. As a workaround, disable app text.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-p7g9-x25m-4h87, https://github.com/nextcloud/text/pull/4877	A-NEX-NEXT-181223/844

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-2023-48302		
Affected Version(s): From (including) 26.0.0 Up to (including) 26.0.8					
N/A	21-Nov-2023	5.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and Nextcloud Enterprise Server, an attacker could insert links into circles name that would be opened when clicking the circle name in a search filter. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.13, 26.0.8, and 27.1.3 contain a fix for this issue. As a workaround, disable app circles. **CVE ID : CVE-2023-48301**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-wgpw-qqq2-gwv6, https://github.com/nextcloud/circles/pull/1415	A-NEX-NEXT-181223/845
Affected Version(s): From (including) 27.0.0 Up to (excluding) 27.1.0					
Server-Side Request Forgery (SSRF)	21-Nov-2023	9.8	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8f69-f9jg-4x3v,	A-NEX-NEXT-181223/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and starting in version 22.0.0 and prior to versions 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Enterprise Server, the DNS pin middleware was vulnerable to DNS rebinding allowing an attacker to perform SSRF as a final result. Nextcloud Server 25.0.11, 26.0.6, and 27.1.0 and Nextcloud Enterprise Server 22.2.10.16, 23.0.12.11, 24.0.12.7, 25.0.11, 26.0.6, and 27.1.0 contain patches for this issue. No known workarounds are available. **CVE ID : CVE-2023-48306**	https://github.com/nextcloud/server/pull/40234	
N/A	21-Nov-2023	4.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-35p6-4992-w5fr,	A-NEX-NEXT-181223/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior to versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and Nextcloud Enterprise Server, when the log level was set to debug, the user_ldap app logged user passwords in plaintext into the log file. If the log file was then leaked or shared in any way the users' passwords would be leaked. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.11, 26.0.6, and 27.1.0 contain a patch for this issue. As a workaround, change config setting `loglevel` to `1` or higher (should always be higher than 1 in production environments). **CVE ID : CVE-2023-48305**	https://github.com/nextcloud/server/pull/40013	
N/A	21-Nov-2023	2.7	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-2448-44rp-c7hh, https://github.	A-NEX-NEXT-181223/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 25.0.11, 26.0.6, and 27.1.0 of Nextcloud Server and Nextcloud Enterprise Server, admins can change authentication details of user configured external storage. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.11, 26.0.6, and 27.1.0 contain a patch for this issue. No known workarounds are available. **CVE ID : CVE-2023-48303**	com/nextcloud/server/pull/39895	
Affected Version(s): From (including) 27.0.0 Up to (excluding) 27.1.3					
N/A	21-Nov-2023	7.1	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and starting in version 20.0.0 and prior to versions 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-f962-hw26-g267, https://github.com/nextcloud/server/pull/41123	A-NEX-NEXT-181223/849

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
			of Nextcloud Enterprise Server, a malicious user could update any personal or global external storage, making them inaccessible for everyone else as well. Nextcloud Server 25.0.13, 26.0.8, and 27.1.3 and Nextcloud Enterprise Server is upgraded to 20.0.14.16, 21.0.9.13, 22.2.10.15, 23.0.12.12, 24.0.12.8, 25.0.13, 26.0.8, and 27.1.3 contain a patch for this issue. As a workaround, disable app files_external. This workaround also makes the external storage inaccessible but retains the configurations until a patched version has been deployed. **CVE ID : CVE-2023-48239**		
N/A	21-Nov-2023	5.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-wgpw-qqq2-gwv6, https://github.	A-NEX-NEXT-181223/850

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
			versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and Nextcloud Enterprise Server, an attacker could insert links into circles name that would be opened when clicking the circle name in a search filter. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.13, 26.0.8, and 27.1.3 contain a fix for this issue. As a workaround, disable app circles. **CVE ID : CVE-2023-48301**	com/nextcloud/circles/pull/1415	
N/A	21-Nov-2023	5.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and Nextcloud Enterprise Server, when a user is tricked into copy pasting HTML code without markup (Ctrl+Shift+V) the markup will actually render.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-p7g9-x25m-4h87, https://github.com/nextcloud/text/pull/4877	A-NEX-NEXT-181223/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Nextcloud Server and Nextcloud Enterprise Server versions 25.0.13, 26.0.8, and 27.1.3 contain a fix for this issue. As a workaround, disable app text. **CVE ID : CVE-2023-48302**		
Affected Version(s): From (including) 27.0.0 Up to (including) 27.1.3					
N/A	21-Nov-2023	5.4	Nextcloud Server provides data storage for Nextcloud, an open source cloud platform. Starting in version 25.0.0 and prior to versions 25.0.13, 26.0.8, and 27.1.3 of Nextcloud Server and Nextcloud Enterprise Server, an attacker could insert links into circles name that would be opened when clicking the circle name in a search filter. Nextcloud Server and Nextcloud Enterprise Server versions 25.0.13, 26.0.8, and 27.1.3 contain a fix for this issue. As a workaround, disable app circles.	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-wgpw-qqq2-gwv6, https://github.com/nextcloud/circles/pull/1415	A-NEX-NEXT-181223/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48301		
Vendor: nkb-bd					
Product: preloader_matrix					
Affected Version(s): * Up to (including) 2.0.1					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Lukman Nakib Preloader Matrix.This issue affects Preloader Matrix: from n/a through 2.0.1. **CVE ID : CVE-2023-47685**	N/A	A-NKB-PREL-181223/853
Vendor: node-openssl_project					
Product: node-openssl					
Affected Version(s): * Up to (including) 2.0.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Nov-2023	9.8	The openssl (aka node-openssl) NPM package through 2.0.0 was characterized as "a nonsense wrapper with no real purpose" by its author, and accepts an opts argument that contains a verb field (used for command execution). NOTE: This vulnerability only affects products that are no longer	https://github.com/ossf/malicious-packages/tree/main/malicious/npm	A-NOD-NODE-181223/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. **CVE ID : CVE-2023-49210**		
Vendor: Nodejs					
Product: node.js					
Affected Version(s): From (including) 16.0.0 Up to (including) 20.6.1					
N/A	23-Nov-2023	7.5	The use of __proto__ in process.mainModule.__proto__.require() can bypass the policy mechanism and require modules outside of the policy.json definition. This vulnerability affects all users using the experimental policy mechanism in all active release lines: v16, v18 and, v20. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js **CVE ID : CVE-2023-30581**	N/A	A-NOD-NODE-181223/855
Vendor: omnisend					
Product: email_marketing_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.13.9					
N/A	23-Nov-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in	N/A	A-OMN-EMAI-181223/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Omnisend Email Marketing for WooCommerce by Omnisend.This issue affects Email Marketing for WooCommerce by Omnisend: from n/a through 1.13.8. **CVE ID : CVE-2023-47244**		
Vendor: opencrx					
Product: opencrx					
Affected Version(s): 5.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-2023	6.1	OpenCRX version 5.2.0 is vulnerable to HTML injection via the Activity Search Criteria-Activity Number. **CVE ID : CVE-2023-40809**	N/A	A-OPE-OPEN-181223/857
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-2023	6.1	OpenCRX version 5.2.0 is vulnerable to HTML injection via Product Name Field. **CVE ID : CVE-2023-40810**	N/A	A-OPE-OPEN-181223/858
Improper Neutralization of Input During Web Page Generation	18-Nov-2023	6.1	OpenCRX version 5.2.0 is vulnerable to HTML injection via the Accounts Group Name Field.	N/A	A-OPE-OPEN-181223/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-40812**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-2023	6.1	OpenCRX version 5.2.0 is vulnerable to HTML injection via Activity Saved Search Creation. **CVE ID : CVE-2023-40813**	N/A	A-OPE-OPEN-181223/860
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-2023	6.1	OpenCRX version 5.2.0 is vulnerable to HTML injection via the Accounts Name Field. **CVE ID : CVE-2023-40814**	N/A	A-OPE-OPEN-181223/861
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-2023	6.1	OpenCRX version 5.2.0 is vulnerable to HTML injection via the Category Creation Name Field. **CVE ID : CVE-2023-40815**	N/A	A-OPE-OPEN-181223/862
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-2023	6.1	OpenCRX version 5.2.0 is vulnerable to HTML injection via Activity Milestone Name Field. **CVE ID : CVE-2023-40816**	N/A	A-OPE-OPEN-181223/863
Improper Neutralization of Input	18-Nov-2023	6.1	OpenCRX version 5.2.0 is vulnerable to HTML injection via the Product	N/A	A-OPE-OPEN-181223/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Configuration Name Field. **CVE ID : CVE-2023-40817**		
Vendor: openharmony					
Product: openharmony					
Affected Version(s): * Up to (including) 3.2.2					
Improper Preservation of Permissions	20-Nov-2023	7.8	in OpenHarmony v3.2.2 and prior versions allow a local attacker arbitrary file read and write through improper preservation of permissions. **CVE ID : CVE-2023-43612**	N/A	A-OPE-OPEN-181223/865
Access of Resource Using Incompatible Type ('Type Confusion')	20-Nov-2023	7.8	in OpenHarmony v3.2.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through type confusion. **CVE ID : CVE-2023-6045**	N/A	A-OPE-OPEN-181223/866
Incorrect Default Permissions	20-Nov-2023	7.1	in OpenHarmony v3.2.2 and prior versions allow a local attacker get confidential information or rewrite sensitive file through incorrect default permissions.	N/A	A-OPE-OPEN-181223/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3116		
Incorrect Default Permissions	20-Nov-2023	5.5	in OpenHarmony v3.2.2 and prior versions allow a local attacker get confidential information through incorrect default permissions. **CVE ID : CVE-2023-42774**	N/A	A-OPE-OPEN-181223/868
Use of Uninitialized Resource	20-Nov-2023	5.5	in OpenHarmony v3.2.2 and prior versions allow a local attacker get sensitive buffer information through use of uninitialized resource. **CVE ID : CVE-2023-46100**	N/A	A-OPE-OPEN-181223/869
Access of Resource Using Incompatible Type ('Type Confusion')	20-Nov-2023	5.5	in OpenHarmony v3.2.2 and prior versions allow a local attacker causes system information leak through type confusion. **CVE ID : CVE-2023-46705**	N/A	A-OPE-OPEN-181223/870
Buffer Copy without Checking Size of Input ('Classic	20-Nov-2023	5.5	in OpenHarmony v3.2.2 and prior versions allow a local attacker cause DOS through buffer overflow.	N/A	A-OPE-OPEN-181223/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID : CVE-2023-47217**		
Vendor: openlinksw					
Product: virtuoso					
Affected Version(s): 7.2.11					
N/A	29-Nov-2023	7.5	An issue in the box_mpy function of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement. **CVE ID : CVE-2023-48946**	https://github.com/openlink/virtuoso-opensource/issues/1178	A-OPE-VIRT-181223/872
N/A	29-Nov-2023	7.5	An issue in the cha_cmp function of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement. **CVE ID : CVE-2023-48947**	https://github.com/openlink/virtuoso-opensource/issues/1179	A-OPE-VIRT-181223/873
N/A	29-Nov-2023	7.5	An issue in the box_div function in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement. **CVE ID : CVE-2023-48948**	https://github.com/openlink/virtuoso-opensource/issues/1176	A-OPE-VIRT-181223/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	29-Nov-2023	7.5	An issue in the box_add function in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement. **CVE ID : CVE-2023-48949**	https://github.com/openlink/virtuoso-opensource/issues/1173	A-OPE-VIRT-181223/875
N/A	29-Nov-2023	7.5	An issue in the box_col_len function in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement. **CVE ID : CVE-2023-48950**	https://github.com/openlink/virtuoso-opensource/issues/1174	A-OPE-VIRT-181223/876
N/A	29-Nov-2023	7.5	An issue in the box_equal function in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) after running a SELECT statement. **CVE ID : CVE-2023-48951**	https://github.com/openlink/virtuoso-opensource/issues/1177	A-OPE-VIRT-181223/877
Deserialization of Untrusted Data	29-Nov-2023	7.5	An issue in the box_deserialize_reusing function in openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of	N/A	A-OPE-VIRT-181223/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) after running a SELECT statement. **CVE ID : CVE-2023-48952**		
Vendor: opennds					
Product: captive_portal					
Affected Version(s): * Up to (excluding) 10.1.2					
Improper Encoding or Escaping of Output	17-Nov-2023	9.8	An issue was discovered in OpenNDS Captive Portal before version 10.1.2. When the custom unescape callback is enabled, attackers can execute arbitrary OS commands by inserting them into the URL portion of HTTP GET requests. **CVE ID : CVE-2023-38316**	https://github.com/openNDS/openNDS/releases/tag/v10.1.2	A-OPE-CAPT-181223/879
NULL Pointer Dereference	17-Nov-2023	7.5	An issue was discovered in OpenNDS Captive Portal before 10.1.2. it has a do_binauth NULL pointer dereference that can be triggered with a crafted GET HTTP request with a missing client redirect query string parameter. Triggering this issue results in crashing openNDS	https://github.com/openNDS/openNDS/releases/tag/v10.1.2	A-OPE-CAPT-181223/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(a Denial-of-Service condition). The issue occurs when the client is about to be authenticated, and can be triggered only when the BinAuth option is set. **CVE ID : CVE-2023-38313**		
NULL Pointer Dereference	17-Nov-2023	7.5	An issue was discovered in OpenNDS Captive Portal before version 10.1.2. It has a try_to_authenticate NULL pointer dereference that can be triggered with a crafted GET HTTP with a missing client token query string parameter. Triggering this issue results in crashing OpenNDS (a Denial-of-Service condition). **CVE ID : CVE-2023-38315**	https://github.com/openNDS/openNDS/releases/tag/v10.1.2	A-OPE-CAPT-181223/881
NULL Pointer Dereference	17-Nov-2023	7.5	An issue was discovered in OpenNDS Captive Portal before version 10.1.2. It has a show_preauthpage NULL pointer dereference that can be triggered	https://github.com/openNDS/openNDS/releases/tag/v10.1.2	A-OPE-CAPT-181223/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with a crafted GET HTTP with a missing User-Agent header. Triggering this issue results in crashing OpenNDS (a Denial-of-Service condition). **CVE ID : CVE-2023-38320**		
NULL Pointer Dereference	17-Nov-2023	7.5	An issue was discovered in OpenNDS Captive Portal before version 10.1.2. It has a do_binauth NULL pointer dereference that be triggered with a crafted GET HTTP request with a missing User-Agent HTTP header. Triggering this issue results in crashing OpenNDS (a Denial-of-Service condition). The issue occurs when the client is about to be authenticated, and can be triggered only when the BinAuth option is set. **CVE ID : CVE-2023-38322**	https://github.com/openNDS/openNDS/releases/tag/v10.1.2	A-OPE-CAPT-181223/883
NULL Pointer Dereference	17-Nov-2023	6.5	An issue was discovered in OpenNDS Captive Portal before version 10.1.2. It has a NULL pointer	https://github.com/openNDS/openNDS/releases/tag/v10.1.2	A-OPE-CAPT-181223/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference in preauthenticated() that can be triggered with a crafted GET HTTP request with a missing redirect query string parameter. Triggering this issue results in crashing OpenNDS (a Denial-of-Service condition). **CVE ID : CVE-2023-38314**		
N/A	17-Nov-2023	5.3	An issue was discovered in OpenNDS Captive Portal before version 10.1.2. It allows users to skip the splash page sequence when it is using the default FAS key and when OpenNDS is configured as FAS (default). **CVE ID : CVE-2023-38324**	https://github.com/openNDS/openNDS/releases/tag/v10.1.2	A-OPE-CAPT-181223/885
Product: opennds					
Affected Version(s): * Up to (excluding) 10.1.3					
Missing Release of Memory after Effective Lifetime	17-Nov-2023	7.5	An issue was discovered in the captive portal in OpenNDS before version 10.1.3. It has multiple memory leaks due to not freeing up allocated memory.	https://github.com/openNDS/openNDS/commit/31dbf4aa069c5bb39a7926d86036ce3b04312b51	A-OPE-OPEN-181223/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This may lead to a Denial-of-Service condition due to the consumption of all available memory. **CVE ID : CVE-2023-41102**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 10.1.3					
Out-of-bounds Write	17-Nov-2023	9.8	An issue was discovered in the captive portal in OpenNDS before version 10.1.3. get_query in http_microhttpd.c does not validate the length of the query string of GET requests. This leads to a stack-based buffer overflow in versions 9.x and earlier, and to a heap-based buffer overflow in versions 10.x and later. Attackers may exploit the issue to crash OpenNDS (Denial-of-Service condition) or to inject and execute arbitrary bytecode (Remote Code Execution). **CVE ID : CVE-2023-41101**	https://github.com/openNDS/openNDS/commit/c294cf30e0a2512062c66e6becb674557b4aed8d	A-OPE-OPEN-181223/887
Vendor: Opennms					
Product: horizon					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 32.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	6.1	Cross-site scripting in bootstrap.jsp in multiple versions of OpenNMS Meridian and Horizon allows an attacker access to confidential session information. The solution is to upgrade to Horizon 32.0.5 or newer and Meridian 2023.1.9 or newer Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be	https://github.com/OpenNMS/opennms/pull/6791	A-OPE-HORI-181223/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directly accessible from the Internet. OpenNMS thanks Moshe Apelbaum for reporting this issue. **CVE ID : CVE-2023-40314**		
Product: meridian					
Affected Version(s): * Up to (excluding) 2023.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	6.1	Cross-site scripting in bootstrap.jsp in multiple versions of OpenNMS Meridian and Horizon allows an attacker access to confidential session information. The solution is to upgrade to Horizon 32.0.5 or newer	https://github.com/OpenNMS/opennms/pull/6791	A-OPE-MERI-181223/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Meridian 2023.1.9 or newer Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet. OpenNMS thanks Moshe Apelbaum for reporting this issue.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40314		
Vendor: openreplay					
Product: openreplay					
Affected Version(s): * Up to (excluding) 1.15.0					
Improper Control of Generation of Code ('Code Injection')	21-Nov-2023	3.5	OpenReplay is a self-hosted session replay suite. In version 1.14.0, due to lack of validation Name field - Account Settings (for registration looks like validation is correct), a bad actor can send emails with HTML injected code to the victims. Bad actors can use this to phishing actions for example. Email is really send from OpenReplay, but bad actors can add there HTML code injected (content spoofing). Please notice that during Registration steps for FullName looks like is validated correct - can not type there, but using this kind of bypass/workaround - bad actors can achieve own goal.	https://github.com/openreplay/openreplay/security/advisories/GHSA-xpfv-454c-3fj4	A-OPE-OPEN-181223/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			As of time of publication, no known fixes or workarounds are available. **CVE ID : CVE-2023-48226**		
Vendor: opensupports					
Product: opensupports					
Affected Version(s): 4.11.0					
Unrestricted Upload of File with Dangerous Type	17-Nov-2023	9.8	OpenSupports v4.11.0 is vulnerable to Unrestricted Upload of File with Dangerous Type. In the comment function, an attacker can bypass security restrictions and upload a .bat file by manipulating the file's magic bytes to masquerade as an allowed type. This can enable the attacker to execute arbitrary code or establish a reverse shell, leading to unauthorized file writes or control over the victim's station via a crafted file upload operation. **CVE ID : CVE-2023-48031**	N/A	A-OPE-OPEN-181223/891
Vendor: openzfs					
Product: openzfs					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.1.13					
Authorization Bypass Through User-Controlled Key	24-Nov-2023	7.5	OpenZFS through 2.1.13 and 2.2.x through 2.2.1, in certain scenarios involving applications that try to rely on efficient copying of file data, can replace file contents with zero-valued bytes and thus potentially disable security mechanisms. NOTE: this issue is not always security related, but can be security related in realistic situations. A possible example is cp, from a recent GNU Core Utilities (coreutils) version, when attempting to preserve a rule set for denying unauthorized access. (One might use cp when configuring access control, such as with the /etc/hosts.deny file specified in the IBM Support reference.) NOTE: this issue occurs less often in version 2.2.1, and in versions before 2.1.4, because of the default	https://github.com/openzfs/zfs/pull/15571, https://github.com/openzfs/zfs/issues/15526, https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=275308, https://news.ycombinator.com/item?id=38405731	A-OPE-OPEN-181223/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration in those versions. **CVE ID : CVE-2023-49298**		
Affected Version(s): 2.2.0					
Authorization Bypass Through User-Controlled Key	24-Nov-2023	7.5	OpenZFS through 2.1.13 and 2.2.x through 2.2.1, in certain scenarios involving applications that try to rely on efficient copying of file data, can replace file contents with zero-valued bytes and thus potentially disable security mechanisms. NOTE: this issue is not always security related, but can be security related in realistic situations. A possible example is cp, from a recent GNU Core Utilities (coreutils) version, when attempting to preserve a rule set for denying unauthorized access. (One might use cp when configuring access control, such as with the /etc/hosts.deny file specified in the IBM Support reference.) NOTE: this issue occurs less often in	https://github.com/openzfs/zfs/pull/15571, https://github.com/openzfs/zfs/issues/15526, https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=275308, https://news.ycombinator.com/item?id=38405731	A-OPE-OPEN-181223/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 2.2.1, and in versions before 2.1.4, because of the default configuration in those versions. **CVE ID : CVE-2023-49298**		
Vendor: os4ed					
Product: opensis					
Affected Version(s): 9.0					
N/A	20-Nov-2023	9.8	The Community Edition version 9.0 of OS4ED's openSIS Classic has a broken access control vulnerability in the database backup functionality. Whenever an admin generates a database backup, the backup is stored in the web root while the file name has a format of "opensisBackup<date>.sql" (e.g. "opensisBackup07-20-2023.sql"), i.e. can easily be guessed. This file can be accessed by any unauthenticated actor and contains a dump of the whole database including password hashes.	N/A	A-OS4-OPEN-181223/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38880		
Cross-Site Request Forgery (CSRF)	20-Nov-2023	8.8	OpenSIS Classic Community Edition version 9.0 lacks cross-site request forgery (CSRF) protection throughout the whole app. This may allow an attacker to trick an authenticated user into performing any kind of state changing request. **CVE ID : CVE-2023-38885**	https://github.com/dub-flow/vulnerability-research/tree/main/CVE-2023-38885	A-OS4-OPEN-181223/895
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Nov-2023	7.5	The Community Edition version 9.0 of OS4ED's openSIS Classic allows remote attackers to read arbitrary files via a directory traversal vulnerability in the 'filename' parameter of 'DownloadWindow.php'. **CVE ID : CVE-2023-38879**	N/A	A-OS4-OPEN-181223/896
Authorization Bypass Through User-Controlled Key	20-Nov-2023	7.5	An Insecure Direct Object Reference (IDOR) vulnerability in the Community Edition version 9.0 of openSIS Classic allows an unauthenticated	https://github.com/dub-flow/vulnerability-research/tree/main/CVE-2023-38884	A-OS4-OPEN-181223/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to access any student's files by visiting '/assets/studentfiles/<studentId>-<filename>' **CVE ID : CVE-2023-38884**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	6.1	A reflected cross-site scripting (XSS) vulnerability in the Community Edition version 9.0 of OS4ED's openSIS Classic allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into any of the 'calendar_id', 'school_date', 'month' or 'year' parameters in 'CalendarModal.php'. **CVE ID : CVE-2023-38881**	https://github.com/dub-flow/vulnerability-research/tree/main/CVE-2023-38881	A-OS4-OPEN-181223/898
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	6.1	A reflected cross-site scripting (XSS) vulnerability in the Community Edition version 9.0 of OS4ED's openSIS Classic allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a	https://github.com/dub-flow/vulnerability-research/tree/main/CVE-2023-38882	A-OS4-OPEN-181223/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious payload into the 'include' parameter in 'ForExport.php' **CVE ID : CVE-2023-38882**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	6.1	A reflected cross-site scripting (XSS) vulnerability in the Community Edition version 9.0 of OS4ED's openSIS Classic allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into the 'ajax' parameter in 'ParentLookup.php' . **CVE ID : CVE-2023-38883**	https://github.com/dub-flow/vulnerability-research/tree/main/CVE-2023-38883	A-OS4-OPEN-181223/900
Vendor: Otrs					
Product: otrs					
Affected Version(s): From (including) 8.0.1 Up to (including) 8.0.37					
Insufficiently Protected Credentials	27-Nov-2023	7.5	A Vulnerability in OTRS AgentInterface and ExternalInterface allows the reading of plain text passwords which are send back to the client in the server response- This issue affects OTRS: from 8.0.X through 8.0.37.	https://otrs.com/release-notes/otrs-security-advisory-2023-11/	A-OTR-OTRS-181223/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6254		
Vendor: Owncloud					
Product: owncloud					
Affected Version(s): * Up to (excluding) 10.13.1					
Improper Authentication	21-Nov-2023	9.8	An issue was discovered in ownCloud owncloud/core before 10.13.1. An attacker can access, modify, or delete any file without authentication if the username of a victim is known, and the victim has no signing-key configured. This occurs because pre-signed URLs can be accepted even when no signing-key is configured for the owner of the files. The earliest affected version is 10.6.0. **CVE ID : CVE-2023-49105**	https://owncloud.com/security-advisories/webdav-api-authentication-bypass-using-pre-signed-urls/	A-OWN-OWNC-181223/902
Vendor: pagerduty					
Product: rundeck					
Affected Version(s): From (including) 4.12.0 Up to (excluding) 4.17.3					
Missing Authorization	16-Nov-2023	5.4	Rundeck is an open source automation service with a web console, command line tools and a	https://github.com/rundeck/rundeck/security/advisories/G	A-PAG-RUND-181223/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WebAPI. In affected versions access to two URLs used in both Rundeck Open Source and Process Automation products could allow authenticated users to access the URL path, which would allow access to view or delete jobs, without the necessary authorization checks. This issue has been addressed in version 4.17.3. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48222**	HSA-phmw-jx86-x666	
Affected Version(s): From (including) 4.17.0 Up to (excluding) 4.17.3					
Missing Authorization	16-Nov-2023	4.3	Rundeck is an open source automation service with a web console, command line tools and a WebAPI. In affected versions access to two URLs used in both Rundeck Open Source and Process Automation products could allow authenticated users to access the	https://github.com/rundeck/rundeck/security/advisories/GHSA-xvmv-4rx6-x6jx	A-PAG-RUND-181223/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URL path, which provides a list of job names and groups for any project, without the necessary authorization checks. The output of these endpoints only exposes the name of job groups and the jobs contained within the specified project. The output is read-only and the access does not allow changes to the information. This vulnerability has been patched in version 4.17.3. Users are advised to upgrade. Users unable to upgrade may block access to the two URLs used in either Rundeck Open Source or Process Automation products at a load balancer level. **CVE ID : CVE-2023-47112**		
Vendor: passionatebrains					
Product: add_expires_headers_\&_optimized_minify					
Affected Version(s): * Up to (including) 2.7					
N/A	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Passionate Brains	N/A	A-PAS-ADD_-181223/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Add Expires Headers & Optimized Minify plugin <= 2.7 versions. **CVE ID : CVE-2023-27457**		
Vendor: patreon					
Product: patreon_wordpress					
Affected Version(s): * Up to (including) 1.8.6					
N/A	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Patreon Patreon WordPress.This issue affects Patreon WordPress: from n/a through 1.8.6. **CVE ID : CVE-2023-41129**	N/A	A-PAT-PATR-181223/906
Vendor: paygreen					
Product: paygreen_-_ancienne					
Affected Version(s): * Up to (including) 4.10.2					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WattIsIt PayGreen – Ancienne version plugin <= 4.10.2 versions. **CVE ID : CVE-2023-25986**	N/A	A-PAY-PAYG-181223/907
Vendor: paymentsplugin					
Product: wp_full_stripe_free					
Affected Version(s): * Up to (including) 1.6.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Mammothology WP Full Stripe Free.This issue affects WP Full Stripe Free: from n/a through 1.6.1. **CVE ID : CVE-2023-47667**	N/A	A-PAY-WP_F-181223/908
Vendor: peachpay					
Product: related_products_for_woocommerce					
Affected Version(s): * Up to (including) 3.3.15					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	The Related Products for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'woo-related' shortcode in versions up to, and including, 3.3.15 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute	https://plugins.trac.wordpress.org/changeset/2988185/woo-related-products-refresh-on-reload	A-PEA-RELA-181223/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			whenever a user accesses an injected page. **CVE ID : CVE-2023-5234**		
Vendor: peepso					
Product: peepso					
Affected Version(s): * Up to (excluding) 6.2.0.0					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in PeepSo Download Community by PeepSo plugin <= 6.1.6.0 versions. **CVE ID : CVE-2023-39925**	N/A	A-PEE-PEEP-181223/910
Vendor: perfops					
Product: decalog					
Affected Version(s): * Up to (including) 3.7.0					
N/A	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Pierre Lannoy / PerfOps One DecaLog plugin <= 3.7.0 versions. **CVE ID : CVE-2023-27444**	N/A	A-PER-DECA-181223/911
Vendor: petersterling					
Product: add_local_avatar					
Affected Version(s): * Up to (including) 12.1					
N/A	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Peter Sterling Add Local Avatar.This issue affects Add	N/A	A-PET-ADD_-181223/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Local Avatar: from n/a through 12.1. **CVE ID : CVE-2023-47650**		
Vendor: phpgurukul					
Product: nipah_virus_testing_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Nov-2023	6.1	A vulnerability classified as problematic has been found in PHPGurukul Nipah Virus Testing Management System 1.0. This affects an unknown part of the file patient-search-report.php of the component Search Report Page. The manipulation of the argument Search By Patient Name with the input <script>alert(document.cookie)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-246123.	N/A	A-PHP-NIPA-181223/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6297		
Vendor: pixelgrade					
Product: customify					
Affected Version(s): * Up to (including) 2.10.4					
N/A	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Pixelgrade Customify – Intuitive Website Styling plugin <= 2.10.4 versions. **CVE ID : CVE-2023-27633**	N/A	A-PIX-CUST-181223/914
Vendor: plainviewplugins					
Product: plainview_protect_passwords					
Affected Version(s): * Up to (including) 1.4					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in edward_plainview Plainview Protect Passwords.This issue affects Plainview Protect Passwords: from n/a through 1.4. **CVE ID : CVE-2023-47664**	N/A	A-PLA-PLAI-181223/915
Vendor: plerdy					
Product: heatmap					
Affected Version(s): * Up to (including) 1.3.2					
Improper Neutralization of	22-Nov-2023	4.8	The Website Optimization – Plerdy plugin for	https://plugins.trac.wordpress.org/browser/p	A-PLE-HEAT-181223/916

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
Input During Web Page Generation ('Cross-site Scripting')			WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's tracking code settings in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-5715**	lerdy-heatmap/trunk/plerdy_heatmap_tracking.php#L132, https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2989840%40plerdy-heatmap&new=2989840%40plerdy-heatmap&sfp_email=&sfph_mail=	
Vendor: popozure					
Product: pz-linkcard					
Affected Version(s): * Up to (including) 2.4.8					
Cross-Site Request Forgery (CSRF)	23-Nov-2023	6.1	Cross-Site Request Forgery (CSRF) leading to Cross-Site Scripting (XSS) vulnerability in Poporon Pz-LinkCard plugin <= 2.4.8 versions.	N/A	A-POP-PZ-L-181223/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47790		
Vendor: precisionbridge					
Product: precision_bridge					
Affected Version(s): * Up to (excluding) 7.3.21					
Improper Certificate Validation	26-Nov-2023	9.1	Precision Bridge PrecisionBridge.exe (aka the thick client) before 7.3.21 allows an integrity violation in which the same license key is used on multiple systems, via vectors involving a Process Hacker memory dump, error message inspection, and modification of a MAC address. **CVE ID : CVE-2023-49312**	N/A	A-PRE-PREC-181223/918
Vendor: prefect					
Product: prefect					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	16-Nov-2023	8.8	An attacker is able to steal secrets and potentially gain remote code execution via CSRF using the open source Prefect web server's API. **CVE ID : CVE-2023-6022**	N/A	A-PRE-PREF-181223/919
Vendor: premio					
Product: chaty					
Affected Version(s): * Up to (excluding) 3.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	4.8	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Premio Chaty plugin <= 3.1.2 versions. **CVE ID : CVE-2023-47759**	N/A	A-PRE-CHAT-181223/920
Product: mystickymenu					
Affected Version(s): * Up to (excluding) 2.6.5					
Incorrect Authorization	20-Nov-2023	5.4	The myStickymenu WordPress plugin before 2.6.5 does not adequately authorize some ajax calls, allowing any logged-in user to perform the actions. **CVE ID : CVE-2023-5509**	N/A	A-PRE-MYST-181223/921
Vendor: pricelisto					
Product: best_restaurant_menu					
Affected Version(s): * Up to (including) 1.3.1					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in PriceListo Best Restaurant Menu by PriceListo.This issue affects Best Restaurant Menu by PriceListo: from n/a through 1.3.1.	N/A	A-PRI-BEST-181223/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47649		
Vendor: publiccms					
Product: publiccms					
Affected Version(s): 4.0.202302.e					
Deserialization of Untrusted Data	20-Nov-2023	9.8	Deserialization of Untrusted Data in PublicCMS v.4.0.202302.e allows a remote attacker to execute arbitrary code via a crafted script to the writeReplace function. **CVE ID : CVE-2023-46990**	N/A	A-PUB-PUBL-181223/923
Server-Side Request Forgery (SSRF)	16-Nov-2023	6.5	An issue in PublicCMS v.4.0.202302.e allows a remote attacker to obtain sensitive information via the appToken and Parameters parameter of the api/method/getHtml component. **CVE ID : CVE-2023-48204**	N/A	A-PUB-PUBL-181223/924
Vendor: pubydoc					
Product: pubydoc					
Affected Version(s): * Up to (including) 2.0.6					
Improper Neutralization of Input During Web Page	20-Nov-2023	4.8	The PubyDoc WordPress plugin through 2.0.6 does not sanitise and escape some of its settings, which	N/A	A-PUB-PUBY-181223/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed **CVE ID : CVE-2023-4970**		
Vendor: pytorch					
Product: torchserve					
Affected Version(s): From (including) 0.1.0 Up to (excluding) 0.9.0					
N/A	21-Nov-2023	5.3	TorchServe is a tool for serving and scaling PyTorch models in production. Starting in version 0.1.0 and prior to version 0.9.0, using the model/workflow management API, there is a chance of uploading potentially harmful archives that contain files that are extracted to any location on the filesystem that is within the process permissions. Leveraging this issue could aid third-party actors in hiding harmful code in open-source/public models, which can be downloaded	https://github.com/pytorch/serve/security/advisories/GHSA-m2mj-pr4f-h9jp, https://github.com/pytorch/serve/pull/2634, https://github.com/pytorch/serve/commit/bfb3d42396727614aef625143b4381e64142f9bb	A-PYT-TORC-181223/926

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
			from the internet, and take advantage of machines running Torchserve. The ZipSlip issue in TorchServe has been fixed by validating the paths of files contained within a zip archive before extracting them. TorchServe release 0.9.0 includes fixes to address the ZipSlip vulnerability. **CVE ID : CVE-2023-48299**		
Vendor: quizandsurveymaster					
Product: quiz_and_survey_master					
Affected Version(s): * Up to (including) 8.1.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ExpressTech Quiz And Survey Master plugin <= 8.1.13 versions. **CVE ID : CVE-2023-47834**	N/A	A-QUI-QUIZ-181223/927
Vendor: Radare					
Product: radare2					
Affected Version(s): * Up to (excluding) 5.9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-Nov-2023	7.5	radare2 5.8.9 has an out-of-bounds read in r_bin_object_set_items in libr/bin/bobj.c, causing a crash in r_read_le32 in libr/include/r_endian.h. **CVE ID : CVE-2023-47016**	https://github.com/radareorg/radare2/issues/22349, https://github.com/radareorg/radare2/commit/40c9f50e127be80b9d816bce2ab2ee790831aefd	A-RAD-RADA-181223/928
Vendor: ray_project					
Product: ray					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Nov-2023	9.8	A command injection exists in Ray's cpu_profile URL parameter allowing attackers to execute os commands on the system running the ray dashboard remotely without authentication. **CVE ID : CVE-2023-6019**	N/A	A-RAY-RAY-181223/929
Missing Authorization	16-Nov-2023	7.5	LFI in Ray's /static/ directory allows attackers to read any file on the server without authentication. **CVE ID : CVE-2023-6020**	N/A	A-RAY-RAY-181223/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Nov-2023	7.5	LFI in Ray's log API endpoint allows attackers to read any file on the server without authentication. **CVE ID : CVE-2023-6021**	N/A	A-RAY-RAY-181223/931
Vendor: razormist					
Product: loan_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Nov-2023	7.2	A vulnerability has been found in SourceCodester Loan Management System 1.0 and classified as critical. This vulnerability affects the function delete_borrower of the file deleteBorrower.php. The manipulation of the argument borrower_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-246136. **CVE ID : CVE-2023-6310**	N/A	A-RAZ-LOAN-181223/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Nov-2023	7.2	A vulnerability was found in SourceCodester Loan Management System 1.0 and classified as critical. This issue affects the function delete_ltype of the file delete_ltype.php of the component Loan Type Page. The manipulation of the argument ltype_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-246137 was assigned to this vulnerability. **CVE ID : CVE-2023-6311**	N/A	A-RAZ-LOAN-181223/933
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Nov-2023	7.2	A vulnerability was found in SourceCodester Loan Management System 1.0. It has been classified as critical. Affected is the function delete_user of the file deleteUser.php of the component Users Page. The manipulation of the argument user_id	N/A	A-RAZ-LOAN-181223/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-246138 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-6312**		
Vendor: redislabs					
Product: redisgraph					
Affected Version(s): 2.12.10					
NULL Pointer Dereference	16-Nov-2023	9.8	An issue in RedisGraph v.2.12.10 allows an attacker to execute arbitrary code and cause a denial of service via a crafted string in DataBlock_ItemIsDeleted. **CVE ID : CVE-2023-47003**	N/A	A-RED-REDI-181223/935
Vendor: rednao					
Product: donations_made_easy_-_smart_donations					
Affected Version(s): * Up to (including) 4.0.12					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in RedNao Donations Made Easy – Smart Donations.This issue affects Donations Made Easy – Smart	N/A	A-RED-DONA-181223/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Donations: from n/a through 4.0.12. **CVE ID : CVE-2023-47551**		
Vendor: remyandrade					
Product: sticky_notes_app					
Affected Version(s): 1.0					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	6.5	A Cross-Site Request Forgery (CSRF) vulnerability in Sourcecodester Sticky Notes App Using PHP with Source Code v.1.0 allows a local attacker to obtain sensitive information via a crafted payload to add-note.php. **CVE ID : CVE-2023-47014**	N/A	A-REM-STIC-181223/937
Vendor: s-sols					
Product: seraphinite_accelerator					
Affected Version(s): * Up to (excluding) 2.2.29					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	6.1	The Seraphinite Accelerator WordPress plugin before 2.2.29 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used	N/A	A-S-S-SERA-181223/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against high privilege users such as admin **CVE ID : CVE-2023-5609**		
URL Redirection to Untrusted Site ('Open Redirect')	20-Nov-2023	5.4	The Seraphinite Accelerator WordPress plugin before 2.2.29 does not validate the URL to redirect any authenticated user to, leading to an arbitrary redirect **CVE ID : CVE-2023-5610**	N/A	A-S-S-SERA-181223/939
Vendor: salesagility					
Product: suitecrm					
Affected Version(s): 8.4.1					
N/A	21-Nov-2023	5.3	SuiteCRM is a Customer Relationship Management (CRM) software application. Prior to version 8.4.2, Graphql Introspection is enabled without authentication, exposing the scheme defining all object types, arguments, and functions. An attacker can obtain the GraphQL schema and understand the entire attack surface of the API, including sensitive	https://github.com/salesagility/SuiteCRM-Core/security/advisories/GHSA-fxww-jqfv-9rrr, https://github.com/salesagility/SuiteCRM-Core/commit/117dd8172793a239f71c91222606bf00677eeb33	A-SAL-SUIT-181223/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fields such as UserHash. This issue is patched in version 8.4.2. There are no known workarounds. **CVE ID : CVE-2023-47643**		
Vendor: seattlelab					
Product: slmail					
Affected Version(s): 5.5.0.4433					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	6.5	Path traversal vulnerability whose exploitation could allow an authenticated remote user to bypass SecurityManager's intended restrictions and list a parent directory via any filename, such as a multiple ..%2F value affecting the 'dodoc' parameter in the /MailAdmin_dll.htm file. **CVE ID : CVE-2023-4593**	N/A	A-SEA-SLMA-181223/941
Insertion of Sensitive Information into Externally-Accessible File or Directory	23-Nov-2023	6.5	An information exposure vulnerability has been found, the exploitation of which could allow a remote user to retrieve sensitive information stored on the server such	N/A	A-SEA-SLMA-181223/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as credential files, configuration files, application files, etc., simply by appending any of the following parameters to the end of the URL: %00 %0a, %20, %2a, %a0, %aa, %c0 and %ca. **CVE ID : CVE-2023-4595**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	5.4	Stored XSS vulnerability. This vulnerability could allow an attacker to store a malicious JavaScript payload via GET and POST methods on multiple parameters in the MailAdmin_dll.htm file. **CVE ID : CVE-2023-4594**	N/A	A-SEA-SLMA-181223/943
Vendor: sequelizejs					
Product: sequelize-typescript					
Affected Version(s): * Up to (excluding) 2.1.6					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	24-Nov-2023	7.1	Prototype Pollution in GitHub repository robinbuschmann/sequelize-typescript prior to 2.1.6. **CVE ID : CVE-2023-6293**	https://huntr.com/bounties/36a7ecbf-4d3d-462e-86a3-cda7b1ec64e2, https://github.com/robinbuschmann/sequelize-typescript/commit/5ce8afdd1671b08c774ce	A-SEQ-SEQU-181223/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				106b000605ba 8fccf78	
Vendor: slimndap					
Product: theater_for_wordpress					
Affected Version(s): * Up to (including) 0.18.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	4.8	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeroen Schmit Theater for WordPress plugin <= 0.18.3 versions. **CVE ID : CVE-2023-47833**	N/A	A-SLI-THEA-181223/945
Vendor: so-wp					
Product: pinyin_slugs					
Affected Version(s): * Up to (including) 2.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in SO WP Pinyin Slugs plugin <= 2.3.0 versions. **CVE ID : CVE-2023-47511**	N/A	A-SO--PINY-181223/946
Vendor: spaceapplications					
Product: yacms					
Affected Version(s): 5.8.6					
Improper Restriction of Rendered UI Layers or Frames	20-Nov-2023	6.1	An issue in Yamcs 5.8.6 allows attackers to send aribitrary telelcommands in a	N/A	A-SPA-YACM-181223/947

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
			Command Stack via Clickjacking. **CVE ID : CVE-2023-47311**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	5.4	Cross Site Scripting vulnerability in Space Applications Services Yamcs v.5.8.6 allows a remote attacker to execute arbitrary code via crafted telecommand in the timeline view of the ArchiveBrowser. **CVE ID : CVE-2023-46470**	N/A	A-SPA-YACM-181223/948
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	5.4	Cross Site Scripting vulnerability in Space Applications Services Yamcs v.5.8.6 allows a remote attacker to execute arbitrary code via the text variable scriptContainer of the ScriptViewer. **CVE ID : CVE-2023-46471**	N/A	A-SPA-YACM-181223/949
Vendor: Splunk					
Product: cloud					
Affected Version(s): * Up to (excluding) 9.1.2308					
XML Injection (aka Blind XPath Injection)	16-Nov-2023	8.8	In Splunk Enterprise versions below 9.0.7 and 9.1.2, Splunk Enterprise does not safely sanitize extensible stylesheet language	https://advisory.splunk.com/advisories/SVD-2023-1104, https://research.splunk.com/application/a053e6a6-2146-	A-SPL-CLOU-181223/950

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
			transformations (XSLT) that users supply. This means that an attacker can upload malicious XSLT which can result in remote code execution on the Splunk Enterprise instance. **CVE ID : CVE-2023-46214**	483a-9798-2d43652f3299/, https://research.splunk.com/application/6cb7e011-55fb-48e3-a98d-164fa854e37e/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	4.8	In Splunk Enterprise versions below 9.0.7 and 9.1.2, ineffective escaping in the “Show syntax Highlighted” feature can result in the execution of unauthorized code in a user’s web browser. **CVE ID : CVE-2023-46213**	https://advisory.splunk.com/advisories/SVD-2023-1103, https://research.splunk.com/application/1030bc63-0b37-4ac9-9ae0-9361c955a3cc/	A-SPL-CLOU-181223/951
Product: splunk					
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.7					
XML Injection (aka Blind XPath Injection)	16-Nov-2023	8.8	In Splunk Enterprise versions below 9.0.7 and 9.1.2, Splunk Enterprise does not safely sanitize extensible stylesheet language transformations (XSLT) that users supply. This means that an attacker can upload malicious XSLT which can	https://advisory.splunk.com/advisories/SVD-2023-1104, https://research.splunk.com/application/a053e6a6-2146-483a-9798-2d43652f3299/, https://research.splunk.com/application/6cb	A-SPL-SPLU-181223/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in remote code execution on the Splunk Enterprise instance. **CVE ID : CVE-2023-46214**	7e011-55fb-48e3-a98d-164fa854e37e/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	4.8	In Splunk Enterprise versions below 9.0.7 and 9.1.2, ineffective escaping in the “Show syntax Highlighted” feature can result in the execution of unauthorized code in a user’s web browser. **CVE ID : CVE-2023-46213**	https://advisory.splunk.com/advisories/SVD-2023-1103, https://research.splunk.com/application/1030bc63-0b37-4ac9-9ae0-9361c955a3cc/	A-SPL-SPLU-181223/953
Affected Version(s): From (including) 9.1.0 Up to (excluding) 9.1.2					
XML Injection (aka Blind XPath Injection)	16-Nov-2023	8.8	In Splunk Enterprise versions below 9.0.7 and 9.1.2, Splunk Enterprise does not safely sanitize extensible stylesheet language transformations (XSLT) that users supply. This means that an attacker can upload malicious XSLT which can result in remote code execution on the Splunk Enterprise instance. **CVE ID : CVE-2023-46214**	https://advisory.splunk.com/advisories/SVD-2023-1104, https://research.splunk.com/application/a053e6a6-2146-483a-9798-2d43652f3299/, https://research.splunk.com/application/6cb7e011-55fb-48e3-a98d-164fa854e37e/	A-SPL-SPLU-181223/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	4.8	In Splunk Enterprise versions below 9.0.7 and 9.1.2, ineffective escaping in the “Show syntax Highlighted” feature can result in the execution of unauthorized code in a user’s web browser. **CVE ID : CVE-2023-46213**	https://advisory.splunk.com/advisories/SVD-2023-1103, https://research.splunk.com/application/1030bc63-0b37-4ac9-9ae0-9361c955a3cc/	A-SPL-SPLU-181223/955
Vendor: star-emea					
Product: star_cloudprnt_for_woocommerce					
Affected Version(s): * Up to (including) 2.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in lawrenceowen, gcubero, acunnningham, fmahmood Star CloudPRNT for WooCommerce plugin <= 2.0.3 versions. **CVE ID : CVE-2023-47514**	N/A	A-STA-STAR-181223/956
Vendor: statamic					
Product: statamic					
Affected Version(s): * Up to (excluding) 3.4.15					
N/A	21-Nov-2023	6.1	Statamic CMS is a Laravel and Git powered content management system (CMS). Prior to versions 3.4.15 an 4.36.0, HTML files crafted to look	https://github.com/statamic/cms/security/advisories/GHSA-8jjh-j3c2-cjcv	A-STA-STAT-181223/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			like images may be uploaded regardless of mime validation. This is only applicable on front-end forms using the "Forms" feature containing an assets field, or within the control panel which requires authentication. This issue has been patched on 3.4.15 and 4.36.0. **CVE ID : CVE-2023-48701**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.36.0					
N/A	21-Nov-2023	6.1	Statamic CMS is a Laravel and Git powered content management system (CMS). Prior to versions 3.4.15 an 4.36.0, HTML files crafted to look like images may be uploaded regardless of mime validation. This is only applicable on front-end forms using the "Forms" feature containing an assets field, or within the control panel which requires authentication. This issue has been patched on 3.4.15 and 4.36.0.	https://github.com/statamic/cms/security/advisories/GHSA-8jjh-j3c2-cjcv	A-STA-STAT-181223/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48701		
Vendor: stevenhenty					
Product: drop_shadow_boxes					
Affected Version(s): * Up to (including) 1.7.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	The Drop Shadow Boxes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'dropshadowbox' shortcode in versions up to, and including, 1.7.13 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5469**	https://plugins.trac.wordpress.org/browser/drop-shadow-boxes/tags/1.7.12/dropshadowboxes.php#L319, https://plugins.trac.wordpress.org/changeset/2998610/drop-shadow-boxes#file1	A-STE-DROP-181223/959
Vendor: store-opart					
Product: op\'art_devis					
Affected Version(s): From (including) 4.5.18 Up to (including) 4.6.12					
Improper Neutralization of	27-Nov-2023	9.8	SQL injection vulnerability in PrestaShop	N/A	A-STO-OP\'-181223/960

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
Special Elements used in an SQL Command ('SQL Injection')			opartdevis v.4.5.18 thru v.4.6.12 allows a remote attacker to execute arbitrary code via a crafted script to the getModuleTranslation function. **CVE ID : CVE-2023-48188**		
Vendor: strangerstudios					
Product: paid_memberships_pro					
Affected Version(s): * Up to (including) 2.12.3					
Unrestricted Upload of File with Dangerous Type	18-Nov-2023	8.8	The Paid Memberships Pro plugin for WordPress is vulnerable to arbitrary file uploads to insufficient file type validation in the 'pmpro_paypalexpress_session_vars_for_user_fields' function in versions up to, and including, 2.12.3. This makes it possible for authenticated attackers with subscriber privileges or above, to upload arbitrary files on the affected site's server which may make remote code execution possible. This can be exploited if 2Checkout	https://www.wordfence.com/threat-intel/vulnerabilities/id/5979f2eb-2ca8-4b06-814c-c4236bb81af0?source=cve, https://plugins.trac.wordpress.org/changeset/2997319/paid-memberships-pro/tags/2.12.4/includes/functions.php	A-STR-PAID-181223/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(deprecated since version 2.6) or PayPal Express is set as the payment method and a custom user field is added that is only visible at profile, and not visible at checkout according to its settings. **CVE ID : CVE-2023-6187**		
Vendor: strapi					
Product: protected_populate					
Affected Version(s): * Up to (excluding) 1.3.4					
N/A	20-Nov-2023	5.3	The Strapi Protected Populate Plugin protects `get` endpoints from revealing too much information. Prior to version 1.3.4, users were able to bypass the field level security. Users who tried to populate something that they didn't have access to could populate those fields anyway. This issue has been patched in version 1.3.4. There are no known workarounds. **CVE ID : CVE-2023-48218**	https://github.com/strapi-community/strapi-plugin-protected-populate/security/advisories/GHSA-6h67-934r-82g7, https://github.com/strapi-community/strapi-plugin-protected-populate/commit/05441066d64e09dd55937d9f089962e9ebe2fb39	A-STR-PROT-181223/962
Vendor: struktur					
Product: libde265					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0.12					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Nov-2023	8.1	Libde265 v1.0.12 was discovered to contain multiple buffer overflows via the num_tile_columns and num_tile_row parameters in the function pic_parameter_set::dump. **CVE ID : CVE-2023-43887**	https://github.com/strukturag/libde265/issues/418, https://github.com/strukturag/libde265/commit/63b596c915977f038eafd7647d1db25488a8c133	A-STR-LIBD-181223/963
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Nov-2023	6.5	Buffer Overflow vulnerability in strukturag libde265 v1.10.12 allows a local attacker to cause a denial of service via the slice_segment_header function in the slice.cc component. **CVE ID : CVE-2023-47471**	https://github.com/strukturag/libde265/issues/426, https://github.com/strukturag/libde265/commit/e36b4a1b0bafa53df47514c419d5be3e8916ebc7	A-STR-LIBD-181223/964
Vendor: superagi					
Product: superagi					
Affected Version(s): 0.0.13					
Use of Hard-coded Credentials	16-Nov-2023	7.5	SuperAGI v0.0.13 was discovered to use a hardcoded key for encryption operations. This vulnerability can lead to the disclosure of information and communications.	N/A	A-SUP-SUPE-181223/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48055		
Vendor: sureshkumarmukhiya					
Product: anywhere_flash_embed					
Affected Version(s): * Up to (including) 1.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Suresh KUMAR Mukhiya Anywhere Flash Embed plugin <= 1.0.5 versions. **CVE ID : CVE-2023-47811**	N/A	A-SUR-ANYW-181223/966
Vendor: swashata					
Product: wp_category_post_list_widget					
Affected Version(s): * Up to (including) 2.0.3					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Swashata WP Category Post List Widget.This issue affects WP Category Post List Widget: from n/a through 2.0.3. **CVE ID : CVE-2023-47672**	N/A	A-SWA-WP_C-181223/967
Vendor: swiftyedit					
Product: swiftyedit					
Affected Version(s): * Up to (excluding) 1.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	SwiftyEdit Content Management System prior to v1.2.0 is vulnerable to Cross Site Request Forgery (CSRF). **CVE ID : CVE-2023-47350**	https://github.com/SwiftyEdit/SwiftyEdit/commit/90a6f3df16cd1578b2827d7b2e073451f7ce4e47	A-SWI-SWIF-181223/968
Vendor: switchwp					
Product: wp_client_reports					
Affected Version(s): * Up to (excluding) 1.0.17					
N/A	23-Nov-2023	6.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in SwitchWP WP Client Reports plugin <= 1.0.16 versions. **CVE ID : CVE-2023-23978**	N/A	A-SWI-WP_C-181223/969
Vendor: Sysaid					
Product: sysaid					
Affected Version(s): * Up to (excluding) 23.2.15					
Authorization Bypass Through User-Controlled Key	24-Nov-2023	6.5	SysAid before 23.2.15 allows Indirect Object Reference (IDOR) attacks to read ticket data via a modified sid parameter to EmailHtmlSourceIframe.jsp or a modified srID parameter to ShowMessage.jsp.	N/A	A-SYS-SYSA-181223/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33706		
Affected Version(s): * Up to (excluding) 23.2.50					
Authorization Bypass Through User-Controlled Key	24-Nov-2023	6.5	SysAid before 23.2.15 allows Indirect Object Reference (IDOR) attacks to read ticket data via a modified sid parameter to EmailHtmlSourceIframe.jsp or a modified srID parameter to ShowMessage.jsp. **CVE ID : CVE-2023-33706**	N/A	A-SYS-SYSA-181223/971
Vendor: tcd-theme					
Product: tcd_google_maps					
Affected Version(s): * Up to (including) 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	The TCD Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'map' shortcode in versions up to, and including, 1.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web	N/A	A-TCD-TCD_-181223/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5128**		
Vendor: techsoupeurope					
Product: leyka					
Affected Version(s): * Up to (including) 3.29.2					
N/A	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Teplitsa of social technologies Leyka plugin <= 3.29.2 versions. **CVE ID : CVE-2023-27442**	N/A	A-TEC-LEYK-181223/973
Vendor: Tenable					
Product: nessus					
Affected Version(s): * Up to (excluding) 10.4.4					
Out-of-bounds Write	20-Nov-2023	6.5	An arbitrary file write vulnerability exists where an authenticated attacker with privileges on the managing application could alter Nessus Rules variables to overwrite arbitrary files on the remote host, which could lead to a denial of service condition.	https://www.tenable.com/security/tns-2023-41	A-TEN-NESS-181223/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6178		
Affected Version(s): * Up to (excluding) 10.5.7					
Out-of-bounds Write	20-Nov-2023	6.5	An arbitrary file write vulnerability exists where an authenticated, remote attacker with administrator privileges on the Nessus application could alter Nessus Rules variables to overwrite arbitrary files on the remote host, which could lead to a denial of service condition. **CVE ID : CVE-2023-6062**	https://www.tenable.com/security/tns-2023-39, https://www.tenable.com/security/tns-2023-40	A-TEN-NESS-181223/975
Affected Version(s): From (including) 10.6.0 Up to (excluding) 10.6.3					
Out-of-bounds Write	20-Nov-2023	6.5	An arbitrary file write vulnerability exists where an authenticated, remote attacker with administrator privileges on the Nessus application could alter Nessus Rules variables to overwrite arbitrary files on the remote host, which could	https://www.tenable.com/security/tns-2023-39, https://www.tenable.com/security/tns-2023-40	A-TEN-NESS-181223/976

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 a denial of service condition. **CVE ID : CVE-2023-6062**		
Vendor: themeblvd					
Product: theme_blvd_shortcodes					
Affected Version(s): * Up to (including) 1.6.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	The Theme Blvd Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.6.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5338**	N/A	A-THE-THEM-181223/977
Vendor: themeisle					
Product: cloud_templates_\&_patterns_collection					
Affected Version(s): * Up to (excluding) 1.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Nov-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in ThemeIsle Cloud Templates & Patterns collection.This issue affects Cloud Templates & Patterns collection: from n/a through 1.2.2. **CVE ID : CVE-2023-47529**	N/A	A-THE-CLOU-181223/978
Vendor: themepoints					
Product: accordion					
Affected Version(s): * Up to (including) 2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Accordion plugin <= 2.6 versions. **CVE ID : CVE-2023-47809**	N/A	A-THE-ACCO-181223/979
Product: tab_ultimate					
Affected Version(s): * Up to (including) 1.3					
Improper Neutralization of Input During	22-Nov-2023	5.4	The Tab Ultimate plugin for WordPress is vulnerable to Stored Cross-Site	https://plugins.trac.wordpress.org/browser/tabs-pro/trunk/the	A-THE-TAB_-181223/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting via the plugin's shortcodes in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5667**	me/tab-shortcode-ultimate-themes.php?rev=2406144#L87, https://plugins.trac.wordpress.org/changeset/2982005/tabs-pro#file23	
Vendor: Themepunch					
Product: slider_revolution					
Affected Version(s): * Up to (including) 6.6.14					
N/A	20-Nov-2023	5.4	Contributor+ Stored Cross-Site Scripting (XSS) vulnerability in Slider Revolution <= 6.6.14. **CVE ID : CVE-2023-47772**	N/A	A-THE-SLID-181223/981
Vendor: thimpress					
Product: wp_hotel_booking					
Affected Version(s): * Up to (excluding) 2.0.8					
Improper Neutralization of	20-Nov-2023	9.8	The WP Hotel Booking WordPress plugin before 2.0.8	N/A	A-THI-WP_H-181223/982

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
Special Elements used in an SQL Command ('SQL Injection')			does not have authorisation and CSRF checks, as well as does not escape user input before using it in a SQL statement of a function hooked to admin_init, allowing unauthenticated users to perform SQL injections **CVE ID : CVE-2023-5652**		
Incorrect Permission Assignment for Critical Resource	20-Nov-2023	5.4	The WP Hotel Booking WordPress plugin before 2.0.8 does not have authorisation and CSRF checks, as well as does not ensure that the package to be deleted is a package, allowing any authenticated users, such as subscriber to delete arbitrary posts **CVE ID : CVE-2023-5651**	N/A	A-THI-WP_H-181223/983
Incorrect Authorization	20-Nov-2023	5.4	The WP Hotel Booking WordPress plugin before 2.0.8 does not have proper authorisation when deleting a package, allowing Contributor and above roles to	N/A	A-THI-WP_H-181223/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delete posts that do no belong to them **CVE ID : CVE-2023-5799**		
Vendor: thrivethemes					
Product: thrive_themes_builder					
Affected Version(s): * Up to (including) 3.24.2					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Thrive Themes Thrive Theme Builder <= 3.24.2 versions. **CVE ID : CVE-2023-47781**	N/A	A-THR-THRI-181223/985
Vendor: tooltips					
Product: wordpress_tooltips					
Affected Version(s): * Up to (including) 8.2.5					
N/A	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Tomas | Docs | FAQ | Premium Support WordPress Tooltips.This issue affects WordPress Tooltips: from n/a through 8.2.5. **CVE ID : CVE-2023-25985**	N/A	A-TOO-WORD-181223/986
Vendor: trellix					
Product: getsusp					
Affected Version(s): * Up to (excluding) 5.0.0.27					
Improper Privilege	16-Nov-2023	7.8		https://kcm.trellix.com/corpor	A-TRE-GETS-181223/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			An Improper Privilege Management vulnerability in Trellix GetSusp prior to version 5.0.0.27 allows a local, low privilege attacker to gain access to files that usually require a higher privilege level. This is caused by GetSusp not correctly protecting a directory that it creates during execution, allowing an attacker to take over file handles used by GetSusp. As this runs with high privileges, the attacker gains elevated permissions. The file handles are opened as read-only. **CVE ID : CVE-2023-6119**	ate/index?page=content&id=SB10412	
Vendor: tribe29					
Product: checkmk					
Affected Version(s): 2.2.0					
N/A	22-Nov-2023	8.8	Improper neutralization of livestatus command delimiters in the	https://checkmk.com/werk/16221	A-TRI-CHEC-181223/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability timeline in Checkmk <= 2.0.0p39, < 2.1.0p37, and < 2.2.0p15 allows arbitrary livestatus command execution for authorized users. **CVE ID : CVE-2023-6156**		
N/A	22-Nov-2023	8.8	Improper neutralization of livestatus command delimiters in ajax_search in Checkmk <= 2.0.0p39, < 2.1.0p37, and < 2.2.0p15 allows arbitrary livestatus command execution for authorized users. **CVE ID : CVE-2023-6157**	https://checkmk.com/werk/16221	A-TRI-CHEC-181223/989
Cross-Site Request Forgery (CSRF)	24-Nov-2023	3.5	Cross-site Request Forgery (CSRF) in Checkmk < 2.2.0p15, < 2.1.0p37, <= 2.0.0p39 allow an authenticated attacker to delete user-messages for individual users. **CVE ID : CVE-2023-6251**	https://checkmk.com/werk/16224	A-TRI-CHEC-181223/990
Affected Version(s): 2.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Nov-2023	8.8	Improper neutralization of livestatus command delimiters in the availability timeline in Checkmk <= 2.0.0p39, < 2.1.0p37, and < 2.2.0p15 allows arbitrary livestatus command execution for authorized users. **CVE ID : CVE-2023-6156**	https://checkmk.com/werk/16221	A-TRI-CHEC-181223/991
N/A	22-Nov-2023	8.8	Improper neutralization of livestatus command delimiters in ajax_search in Checkmk <= 2.0.0p39, < 2.1.0p37, and < 2.2.0p15 allows arbitrary livestatus command execution for authorized users. **CVE ID : CVE-2023-6157**	https://checkmk.com/werk/16221	A-TRI-CHEC-181223/992
Cross-Site Request Forgery (CSRF)	24-Nov-2023	3.5	Cross-site Request Forgery (CSRF) in Checkmk < 2.2.0p15, < 2.1.0p37, <= 2.0.0p39 allow an authenticated attacker to delete user-messages for individual users.	https://checkmk.com/werk/16224	A-TRI-CHEC-181223/993

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-2023-6251		
Affected Version(s): 2.1.0					
N/A	22-Nov-2023	8.8	Improper neutralization of livestatus command delimiters in the availability timeline in Checkmk <= 2.0.0p39, < 2.1.0p37, and < 2.2.0p15 allows arbitrary livestatus command execution for authorized users. **CVE ID : CVE-2023-6156**	https://checkmk.com/werk/16221	A-TRI-CHEC-181223/994
N/A	22-Nov-2023	8.8	Improper neutralization of livestatus command delimiters in ajax_search in Checkmk <= 2.0.0p39, < 2.1.0p37, and < 2.2.0p15 allows arbitrary livestatus command execution for authorized users. **CVE ID : CVE-2023-6157**	https://checkmk.com/werk/16221	A-TRI-CHEC-181223/995
Cross-Site Request Forgery (CSRF)	24-Nov-2023	3.5	Cross-site Request Forgery (CSRF) in Checkmk < 2.2.0p15, < 2.1.0p37, <= 2.0.0p39 allow an authenticated	https://checkmk.com/werk/16224	A-TRI-CHEC-181223/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to delete user-messages for individual users. **CVE ID : CVE-2023-6251**		
Vendor: ubertidavide					
Product: fastbots					
Affected Version(s): * Up to (excluding) 0.1.5					
Improper Control of Generation of Code ('Code Injection')	21-Nov-2023	9.8	fastbots is a library for fast bot and scraper development using selenium and the Page Object Model (POM) design. Prior to version 0.1.5, an attacker could modify the locators.ini locator file with python code that without proper validation it's executed and it could lead to rce. The vulnerability is in the function `def __locator__(self, locator_name: str)` in `page.py`. In order to mitigate this issue, upgrade to fastbots version 0.1.5 or above. **CVE ID : CVE-2023-48699**	https://github.com/ubertidavide/fastbots/security/advisories/GHSA-vccg-f4gp-45x9, https://github.com/ubertidavide/fastbots/pull/3#issue-2003080806, https://github.com/ubertidavide/fastbots/commit/73eb03bd75365e112b39877e26ef52853f5e9f57	A-UBE-FAST-181223/997
Vendor: url_shortener_project					
Product: url_shortener					
Affected Version(s): 1.0					
Improper Neutralization of	27-Nov-2023	6.1	A vulnerability was found in SourceCodester	N/A	A-URL-URL_-181223/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			URL Shortener 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Long URL Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-246139. **CVE ID : CVE-2023-6313**		
Vendor: urosevic					
Product: my_youtube_channel					
Affected Version(s): * Up to (excluding) 3.23.4					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Aleksandar Uroševi? My YouTube Channel plugin <= 3.23.3 versions. **CVE ID : CVE-2023-25987**	N/A	A-URO-MY_Y-181223/999
Vendor: usedesk					
Product: usedesk					
Affected Version(s): * Up to (excluding) 1.7.57					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Nov-2023	9.8	Usedesk before 1.7.57 allows chat template injection. **CVE ID : CVE-2023-49214**	https://usedesk.ru/updates_september23	A-USE-USED-181223/1000
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	6.1	Usedesk before 1.7.57 allows filter reflected XSS. **CVE ID : CVE-2023-49215**	https://usedesk.ru/updates_september23	A-USE-USED-181223/1001
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	5.4	Usedesk before 1.7.57 allows profile stored XSS. **CVE ID : CVE-2023-49216**	https://usedesk.ru/updates_september23	A-USE-USED-181223/1002
Vendor: userlocal					
Product: userheat_plugin					
Affected Version(s): * Up to (including) 1.1.6					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in User Local Inc UserHeat Plugin.This issue affects UserHeat	N/A	A-USE-USER-181223/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plugin: from n/a through 1.1.6. **CVE ID : CVE-2023-47553**		
Vendor: userproplugin					
Product: userpro					
Affected Version(s): * Up to (excluding) 5.1.2					
N/A	22-Nov-2023	6.5	The UserPro plugin for WordPress is vulnerable to sensitive information disclosure via the 'userpro' shortcode in versions up to, and including 5.1.1. This is due to insufficient restriction on sensitive user meta values that can be called via that shortcode. This makes it possible for authenticated attackers, with subscriber-level permissions, and above to retrieve sensitive user meta that can be used to gain access to a high privileged user account. **CVE ID : CVE-2023-2446**	N/A	A-USE-USER-181223/1004
Cross-Site Request	22-Nov-2023	6.1	The UserPro plugin for WordPress is vulnerable to	N/A	A-USE-USER-181223/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Cross-Site Request Forgery in versions up to, and including, 5.1.1. This is due to missing or incorrect nonce validation on the 'export_users' function. This makes it possible for unauthenticated attackers to export the users to a csv file, granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2447**		
Affected Version(s): * Up to (including) 5.1.1					
Improper Authentication	22-Nov-2023	8.1	The UserPro plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 5.1.1. This is due to insufficient verification on the user being supplied during a Facebook login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if	N/A	A-USE-USER-181223/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they have access to the email. An attacker can leverage CVE-2023-2448 and CVE-2023-2446 to get the user's email address to successfully exploit this vulnerability. **CVE ID : CVE-2023-2437**		
Missing Authorization	22-Nov-2023	6.5	The UserPro plugin for WordPress is vulnerable to unauthorized access of data, modification of data, loss of data due to a missing capability check on multiple functions in all versions up to, and including, 5.1.1. This makes it possible for unauthenticated attackers to add, modify, or delete user meta and plugin options. **CVE ID : CVE-2023-6007**	N/A	A-USE-USER-181223/1007
Cross-Site Request Forgery (CSRF)	22-Nov-2023	4.3	The UserPro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 5.1.1. This is due to missing or incorrect nonce	N/A	A-USE-USER-181223/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation on multiple functions. This makes it possible for unauthenticated attackers to add, modify, or delete user meta and plugin options. **CVE ID : CVE-2023-6008**		
Affected Version(s): * Up to (including) 5.1.4					
N/A	22-Nov-2023	8.8	The UserPro plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 5.1.4 due to insufficient restriction on the 'userpro_update_user_profile' function. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to modify their user role by supplying the 'wp_capabilities' parameter during a profile update. **CVE ID : CVE-2023-6009**	N/A	A-USE-USER-181223/1009
Vendor: venutius					
Product: bp_profile_shortcodes_extra					
Affected Version(s): * Up to (including) 2.5.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Venutius BP Profile Shortcodes Extra plugin <= 2.5.2 versions. **CVE ID : CVE-2023-47815**	N/A	A-VEN-BP_P-181223/1010
Vendor: veom					
Product: service_tracking					
Affected Version(s): * Up to (including) 20231122					
N/A	22-Nov-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Veon Computer Service Tracking Software allows SQL Injection.This issue affects Service Tracking Software: through 20231122. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-VEO-SERV-181223/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2889		
Vendor: veribase					
Product: veribase					
Affected Version(s): * Up to (including) 2023-11-23					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Nov-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Veribilim Software Computer Veribase allows SQL Injection.This issue affects Veribase: through 20231123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3377**	N/A	A-VER-VERI-181223/1012
Vendor: vertaai					
Product: modeldb					
Affected Version(s): -					
Improper Limitation of a Pathname	16-Nov-2023	7.5	An attacker can read any file on the filesystem on the server hosting	N/A	A-VER-MODE-181223/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			ModelDB through an LFI in the artifact_path URL parameter. **CVE ID : CVE-2023-6023**		
Vendor: Videolan					
Product: vlc_media_player					
Affected Version(s): * Up to (excluding) 3.0.19					
Uncontrolled Search Path Element	22-Nov-2023	7.8	A binary hijacking vulnerability exists within the VideoLAN VLC media player before 3.0.19 on Windows. The uninstaller attempts to execute code with elevated privileges out of a standard user writable location. Standard users may use this to gain arbitrary code execution as SYSTEM. **CVE ID : CVE-2023-46814**	https://www.videolan.org/security/sb-vlc3019.html	A-VID-VLC_-181223/1014
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.0.2106					
Use After Free	16-Nov-2023	4.3	Vim is an open source command line text editor. When closing a window, vim may try to access already freed window structure. Exploitation	https://github.com/vim/vim/security/advisories/GHSA-8g46-v9ff-c765, https://github.com/vim/vim/commit/25aab	A-VIM-VIM-181223/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beyond crashing the application has not been shown to be viable. This issue has been addressed in commit `25aabc2b` which has been included in release version 9.0.2106. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48231**	c2b8ee1e19ced6f4da9d866cf9378fc4c5a	
Affected Version(s): * Up to (excluding) 9.0.2107					
Improper Handling of Exceptional Conditions	16-Nov-2023	4.3	Vim is an open source command line text editor. A floating point exception may occur when calculating the line offset for overlong lines and smooth scrolling is enabled and the cpo-settings include the 'n' flag. This may happen when a window border is present and when the wrapped line continues on the next physical line directly in the window border because the 'cpo' setting includes the 'n' flag. Only users with non-default	https://github.com/vim/vim/security/advisories/GHSA-f6cx-x634-hqpw, https://github.com/vim/vim/commit/cb0b99f0672d8446585d26e998343dceca17d1ce	A-VIM-VIM-181223/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			settings are affected and the exception should only result in a crash. This issue has been addressed in commit `cb0b99f0` which has been included in release version 9.0.2107. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48232**		
Affected Version(s): * Up to (excluding) 9.0.2108					
Integer Overflow or Wraparound	16-Nov-2023	4.3	Vim is an open source command line text editor. If the count after the :s command is larger than what fits into a (signed) long variable, abort with e_value_too_large. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `ac6378773` which has been included in release version 9.0.2108. Users are advised to upgrade.	https://github.com/vim/vim/security/advisories/GHSA-3xx4-hcq6-r2vj, https://github.com/vim/vim/commit/ac63787734fda2e294e477af52b3bd601517fa78	A-VIM-VIM-181223/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48233**		
Affected Version(s): * Up to (excluding) 9.0.2109					
Integer Overflow or Wraparound	16-Nov-2023	4.3	Vim is an open source command line text editor. When getting the count for a normal mode z command, it may overflow for large counts given. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `58f9befca1` which has been included in release version 9.0.2109. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48234**	https://github.com/vim/vim/security/advisories/GHSA-59gw-c949-6phq, https://github.com/vim/vim/commit/58f9befca1fa172068effad7f2ea5a9d6a7b0cca	A-VIM-VIM-181223/1018
Affected Version(s): * Up to (excluding) 9.0.2110					
Integer Overflow or Wraparound	16-Nov-2023	4.3	Vim is an open source command line text editor. When parsing relative ex addresses one may	https://github.com/vim/vim/security/advisories/GHSA-6g74-hr6q-pr8g,	A-VIM-VIM-181223/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unintentionally cause an overflow. Ironically this happens in the existing overflow check, because the line number becomes negative and LONG_MAX - lnum will cause the overflow. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `060623e` which has been included in release version 9.0.2110. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48235**	https://github.com/vim/vim/commit/060623e4a3bc72b011e7cd92bedb3bfb64e06200	
Affected Version(s): * Up to (excluding) 9.0.2111					
Integer Overflow or Wraparound	16-Nov-2023	4.3	Vim is an open source command line text editor. When using the z= command, the user may overflow the count with values larger than MAX_INT. Impact is low, user interaction is	https://github.com/vim/vim/security/advisories/GHSA-pr4c-932v-8hx5, https://github.com/vim/vim/commit/73b2d3790cad5694fc	A-VIM-VIM-181223/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			required and a crash may not even happen in all situations. This vulnerability has been addressed in commit `73b2d379` which has been included in release version 9.0.2111. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48236**	0ed0db2926e4220c48d968	
Affected Version(s): * Up to (excluding) 9.0.2112					
Integer Overflow or Wraparound	16-Nov-2023	4.3	Vim is an open source command line text editor. In affected versions when shifting lines in operator pending mode and using a very large value, it may be possible to overflow the size of integer. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `6bf131888` which has been included in version 9.0.2112. Users are advised to upgrade. There	https://github.com/vim/vim/security/advisories/GHSA-f2m2-v387-gv87, https://github.com/vim/vim/commit/6bf131888a3d1de62bbfa8a7ea03c0ddccfd496e	A-VIM-VIM-181223/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48237**		
Vendor: vjinfotech					
Product: woo_custom_and_sequential_order_number					
Affected Version(s): * Up to (including) 2.6.0					
Cross-Site Request Forgery (CSRF)	16-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in VJInfotech Woo Custom and Sequential Order Number plugin <= 2.6.0 versions. **CVE ID : CVE-2023-47687**	N/A	A-VJI-WOO_-181223/1022
Vendor: warpgate_project					
Product: warpgate					
Affected Version(s): * Up to (including) 0.8.1					
Incorrect Authorization	24-Nov-2023	8.8	Warpgate is an open source SSH, HTTPS and MySQL bastion host for Linux. In affected versions there is a privilege escalation vulnerability through a non-admin user's account. Limited users can impersonate another user's account if only single-factor authentication is configured. If a user knows an admin username, opens	https://github.com/warp-tech/warpgate/security/advisories/GHSA-c94j-vqr5-3mxr, https://github.com/warp-tech/warpgate/commit/e3b26b2699257b9482dce2e9157bd9b5e05d9c76	A-WAR-WARP-181223/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the login screen and attempts to authenticate with an incorrect password they can subsequently enter a valid non-admin username and password they will be logged in as the admin user. All installations prior to version 0.9.0 are affected. All users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48712**		
Vendor: wcproducttable					
Product: woocommerce_product_table_lite					
Affected Version(s): * Up to (including) 2.6.2					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WC Product Table WooCommerce Product Table Lite.This issue affects WooCommerce Product Table Lite: from n/a through 2.6.2. **CVE ID : CVE-2023-47519**	N/A	A-WCP-WOOC-181223/1024
Vendor: weather-atlas					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: weather_atlas					
Affected Version(s): * Up to (including) 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	The Weather Atlas Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'shortcode-weather-atlas' shortcode in versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5163**	https://plugins.trac.wordpress.org/browser/weather-atlas/tags/1.2.1/includes/class-weather-atlas.php#L838 , https://plugins.trac.wordpress.org/browser/weather-atlas/tags/1.2.1/includes/class-weather-atlas.php#L858	A-WEA-WEAT-181223/1025
Vendor: Web-dorado					
Product: contact_form_builder					
Affected Version(s): * Up to (including) 1.0.72					
Improper Neutralization of Input During Web Page Generation	22-Nov-2023	5.4	The WDContactFormBuilder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the	N/A	A-WEB-CONT-181223/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			'Contact_Form_Builder' shortcode in versions up to, and including, 1.0.72 due to insufficient input sanitization and output escaping on 'id' user supplied attribute. This makes it possible for authenticated attackers with contributor level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5048**		
Vendor: webdevocean					
Product: image_hover_effects					
Affected Version(s): * Up to (including) 5.5					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Labib Ahmed Image Hover Effects – WordPress Plugin.This issue affects Image Hover Effects – WordPress Plugin: from n/a through 5.5.	N/A	A-WEB-IMAG-181223/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47552		
Vendor: webternsolutions					
Product: video_xml_sitemap_generator					
Affected Version(s): * Up to (including) 1.0.0					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Tradebooster Video XML Sitemap Generator.This issue affects Video XML Sitemap Generator: from n/a through 1.0.0. **CVE ID : CVE-2023-31089**	N/A	A-WEB-VIDE-181223/1028
Vendor: wire					
Product: audio\,_video\,_and_signaling					
Affected Version(s): * Up to (excluding) 9.2.22					
N/A	20-Nov-2023	8.8	wire-avs provides Audio, Visual, and Signaling (AVS) functionality sure the secure messaging software Wire. Prior to versions 9.2.22 and 9.3.5, a remote format string vulnerability could potentially allow an attacker to cause a denial of service or possibly execute arbitrary code. The issue has been fixed in wire-avs 9.2.22 &	https://github.com/wireapp/wire-avs/security/advisories/GHSA-m4xg-fcr3-w3pq, https://github.com/wireapp/wire-avs/commit/364c3326a1331a84607bce2e17126306d39150cd	A-WIR-AUDI-181223/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.3.5 and is already included on all Wire products. No known workarounds are available. **CVE ID : CVE-2023-48221**		
Affected Version(s): From (including) 9.3.0 Up to (including) 9.3.5					
N/A	20-Nov-2023	8.8	wire-avs provides Audio, Visual, and Signaling (AVS) functionality sure the secure messaging software Wire. Prior to versions 9.2.22 and 9.3.5, a remote format string vulnerability could potentially allow an attacker to cause a denial of service or possibly execute arbitrary code. The issue has been fixed in wire-avs 9.2.22 & 9.3.5 and is already included on all Wire products. No known workarounds are available. **CVE ID : CVE-2023-48221**	https://github.com/wireapp/wire-avs/security/advisories/GHSA-m4xg-fcr3-w3pq, https://github.com/wireapp/wire-avs/commit/364c3326a1331a84607bce2e17126306d39150cd	A-WIR-AUDI-181223/1030
Vendor: Wireshark					
Product: wireshark					
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.10					
Improper Neutralization of	16-Nov-2023	6.5	SSH dissector crash in Wireshark 4.0.0 to 4.0.10 allows	https://www.wireshark.org/security/wnpa-	A-WIR-WIRE-181223/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements in Output Used by a Downstream Component ('Injection')			denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-6174**	sec-2023-28.html, https://gitlab.com/wireshark/wireshark/-/issues/19369	
Vendor: wishfulthemes					
Product: raise_mag					
Affected Version(s): * Up to (including) 1.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wishfulthemes Raise Mag, Wishfulthemes Wishful Blog themes allows Reflected XSS.This issue affects Raise Mag: from n/a through 1.0.7; Wishful Blog: from n/a through 2.0.1. **CVE ID : CVE-2023-28621**	N/A	A-WIS-RAIS-181223/1032
Product: wishful_blog					
Affected Version(s): * Up to (including) 2.0.1					
Improper Neutralization of Input	16-Nov-2023	6.1	Improper Neutralization of Input During Web Page Generation	N/A	A-WIS-WISH-181223/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			('Cross-site Scripting') vulnerability in Wishfulthemes Raise Mag, Wishfulthemes Wishful Blog themes allows Reflected XSS.This issue affects Raise Mag: from n/a through 1.0.7; Wishful Blog: from n/a through 2.0.1. **CVE ID : CVE-2023-28621**		
Vendor: wpcharitable					
Product: charitable					
Affected Version(s): * Up to (including) 1.7.0.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Charitable Donations & Fundraising Team Donation Forms by Charitable plugin <= 1.7.0.13 versions. **CVE ID : CVE-2023-47816**	N/A	A-WPC-CHAR-181223/1034
Vendor: wpchill					
Product: cpo_shortcodes					
Affected Version(s): * Up to (including) 1.5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	The CPO Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 1.5.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5704**	https://plugins.trac.wordpress.org/browser/cpo-shortcodes/trunk/shortcodes/shortcode-testimonial.php?rev=2413204#L38	A-WPC-CPO_-181223/1035
Vendor: wpdeveloper					
Product: essential_addons_for_elementor					
Affected Version(s): * Up to (including) 5.4.8					
N/A	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WPDeveloper Essential Addons for Elementor Pro.This issue affects Essential Addons for Elementor Pro:	N/A	A-WPD-ESSE-181223/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a through 5.4.8. **CVE ID : CVE-2023-32245**		
Vendor: wpembedfb					
Product: magic_embeds					
Affected Version(s): * Up to (excluding) 3.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Nov-2023	5.4	The Magic Embeds WordPress plugin before 3.1.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-4799**	N/A	A-WPE-MAGI-181223/1037
Vendor: wpexpertplugins					
Product: post_meta_data_manager					
Affected Version(s): * Up to (excluding) 1.2.2					
Cross-Site Request Forgery (CSRF)	21-Nov-2023	8.8	The Post Meta Data Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.1.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2981559%40post-meta-data-	A-WPE-POST-181223/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This is due to missing nonce validation on the pmdm_wp_ajax_delete_meta, pmdm_wp_delete_user_meta, and pmdm_wp_delete_user_meta functions. This makes it possible for unauthenticated attackers to delete arbitrary user, term, and post meta via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-5776**	manager&new=2981559%40post-meta-data-manager&sfp_email=&sfph_mail=	
Vendor: wpgov					
Product: anac_xml_bandi_di_gara					
Affected Version(s): * Up to (including) 7.5					
Cross-Site Request Forgery (CSRF)	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Marco Milesi ANAC XML Bandi di Gara.This issue affects ANAC XML Bandi di Gara: from n/a through 7.5. **CVE ID : CVE-2023-47655**	N/A	A-WPG-ANAC-181223/1039
Vendor: wphive					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: product_enquiry_for_woocommerce					
Affected Version(s): * Up to (including) 3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Gravity Master Product Enquiry for WooCommerce plugin <= 3.0 versions. **CVE ID : CVE-2023-47512**	N/A	A-WPH-PROD-181223/1040
Vendor: wplinkspage					
Product: wp_links_page					
Affected Version(s): * Up to (including) 4.9.4					
N/A	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Robert Macchi WP Links Page.This issue affects WP Links Page: from n/a through 4.9.4. **CVE ID : CVE-2023-47651**	N/A	A-WPL-WP_L-181223/1041
Vendor: wpplugin					
Product: easy_paypal_shopping_cart					
Affected Version(s): * Up to (including) 1.1.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Scott Paterson Easy PayPal Shopping Cart plugin <= 1.1.10 versions.	N/A	A-WPP-EASY-181223/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47239		
Vendor: wppool					
Product: sheets_to_wp_table_live_sync					
Affected Version(s): * Up to (including) 2.12.15					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WPPOOL Sheets To WP Table Live Sync plugin <= 2.12.15 versions. **CVE ID : CVE-2023-26535**	N/A	A-WPP-SHEE-181223/1043
Vendor: wpsimplesponsorships					
Product: sponsors					
Affected Version(s): * Up to (including) 3.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	5.4	The Sponsors plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sponsors' shortcode in all versions up to, and including, 3.5.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute	https://plugins.trac.wordpress.org/browser/wp-sponsors/tags/3.5.0/includes/class-wp-sponsors-shortcodes.php#L267	A-WPS-SPON-181223/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			whenever a user accesses an injected page. **CVE ID : CVE-2023-5662**		
Vendor: wpstream					
Product: wpstream					
Affected Version(s): * Up to (including) 4.4.10					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in wpstream WpStream plugin <= 4.4.10 versions. **CVE ID : CVE-2023-27458**	N/A	A-WPS-WPST-181223/1045
Vendor: wpvnteam					
Product: wp_extra					
Affected Version(s): * Up to (excluding) 6.5					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in TienCOP WP EXtra plugin <= 6.4 versions. **CVE ID : CVE-2023-47825**	N/A	A-WPV-WP_E-181223/1046
Affected Version(s): * Up to (including) 6.2					
N/A	22-Nov-2023	4.3	The WP EXtra plugin for WordPress is vulnerable to unauthorized access to restricted functionality due to a missing capability check on the 'test-email' section of the register() function	https://plugins.trac.wordpress.org/changeset/2977703/wp-extra	A-WPV-WP_E-181223/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in versions up to, and including, 6.2. This makes it possible for authenticated attackers, with minimal permissions such as a subscriber, to send emails with arbitrary content to arbitrary locations from the affected site's mail server. **CVE ID : CVE-2023-5314**		
Vendor: wpwax					
Product: legal_pages					
Affected Version(s): * Up to (excluding) 1.3.9					
Cross-Site Request Forgery (CSRF)	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in wpWax Legal Pages – Privacy Policy, Terms & Conditions, GDPR, CCPA, and Cookie Notice Generator plugin <= 1.3.8 versions. **CVE ID : CVE-2023-47824**	N/A	A-WPW-LEGA-181223/1048
Vendor: Xwiki					
Product: admin_tools					
Affected Version(s): From (including) 4.4 Up to (excluding) 4.5.1					
N/A	20-Nov-2023	8.8	The XWiki Admin Tools Application provides tools to help the administration of XWiki. Starting in	https://github.com/xwiki-contrib/application-admintools/security/advisorie	A-XWI-ADMI-181223/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	version 4.4 and prior to version 4.5.1, a cross site request forgery vulnerability in the admin tool for executing shell commands on the server allows an attacker to execute arbitrary shell commands by tricking an admin into loading the URL with the shell command. A very simple possibility for an attack are comments. When the attacker can leave a comment on any page in the wiki it is sufficient to include an image with an URL like `/xwiki/bin/view/Admin/RunShellCommand?command=touch%20/tmp/attacked` in the comment. When an admin views the comment, the file `/tmp/attacked` will be created on the server. The output of the command is also vulnerable to XWiki syntax injection which offers a simple way to execute Groovy in the context of the	s/GHSA-8jpr-ff92-hpf9, https://github.com/xwiki-contrib/application-admintools/commit/03815c505c9f37006a0c56495e862dc549a39da8, https://jira.xwiki.org/browse/ADMINTOOL-91	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XWiki installation and thus an even easier way to compromise the integrity and confidentiality of the whole XWiki installation. This has been patched by adding a form token check in version 4.5.1 of the admin tools. Some workarounds are available. The patch can be applied manually to the affected wiki pages. Alternatively, the document `Admin.RunShellCommand` can also be deleted if the possibility to run shell commands isn't needed. **CVE ID : CVE-2023-48292**		
Product: Xwiki					
Affected Version(s): * Up to (excluding) 4.5.1					
N/A	20-Nov-2023	8.8	The XWiki Admin Tools Application provides tools to help the administration of XWiki. Prior to version 4.5.1, a cross-site request forgery vulnerability in the query on XWiki tool allows executing arbitrary database	https://github.com/xwiki-contrib/application-admintools/security/advisories/GHSA-4f4c-rhjv-4wgv, https://github.com/xwiki-contrib/application-admintools/co	A-XWI-XWIK-181223/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			queries on the database of the XWiki installation. Among other things, this allows modifying and deleting all data of the wiki. This could be both used to damage the wiki and to create an account with elevated privileges for the attacker, thus impacting the confidentiality, integrity and availability of the whole XWiki instance. A possible attack vector are comments on the wiki, by embedding an image with wiki syntax like `[[image:path:/xwiki/bin/view/Admin/QueryOnXWiki?query=DELETE%20FROM%20xwikidoc]]`, all documents would be deleted from the database when an admin user views this comment. This has been patched in Admin Tools Application 4.5.1 by adding form token checks. Some workarounds are available. The patch can also be applied	mmit/45298b4fbcafba6914537dcdd798a1e1385f9e46, https://jira.xwiki.org/browse/ADMINTOOL-92	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manually to the affected pages. Alternatively, if the query tool is not needed, by deleting the document `Admin.SQLToolsGroovy`, all database query tools can be deactivated. **CVE ID : CVE-2023-48293**		
Affected Version(s): 15.6					
Server-Side Request Forgery (SSRF)	20-Nov-2023	8.8	XWiki Platform is a generic wiki platform. The rendered diff in XWiki embeds images to be able to compare the contents and not display a difference for an actually unchanged image. For this, XWiki requests all embedded images on the server side. These requests are also sent for images from other domains and include all cookies that were sent in the original request to ensure that images with restricted view right can be compared. Starting in version 11.10.1 and prior to versions 14.10.15, 15.5.1, and 15.6,	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-7rfg-6273-f5wp, https://github.com/xwiki/xwiki-platform/commit/bff0203e739b6e3eb90af5736f04278c73c2a8bb, https://jira.xwiki.org/browse/XWIKI-20818	A-XWI-XWIK-181223/1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this allows an attacker to steal login and session cookies that allow impersonating the current user who views the diff. The attack can be triggered with an image that references the rendered diff, thus making it easy to trigger. Apart from stealing login cookies, this also allows server-side request forgery (the result of any successful request is returned in the image's source) and viewing protected content as once a resource is cached, it is returned for all users. As only successful requests are cached, the cache will be filled by the first user who is allowed to access the resource. This has been patched in XWiki 14.10.15, 15.5.1 and 15.6. The rendered diff now only downloads images from trusted domains. Further, cookies are only sent when the image's domain		

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
			is the same the requested domain. The cache has been changed to be specific for each user. As a workaround, the image embedding feature can be disabled by deleting `xwiki-platform-diff-xml-<version>.jar` in `WEB-INF/lib/`. **CVE ID : CVE-2023-48240**		
Affected Version(s): 6.3					
N/A	20-Nov-2023	7.5	XWiki Platform is a generic wiki platform. Starting in version 6.3-milestone-2 and prior to versions 14.10.15, 15.5.1, and 15.6RC1, the Solr-based search suggestion provider that also duplicates as generic JavaScript API for search results in XWiki exposes the content of all documents of all wikis to anybody who has access to it, by default it is public. This exposes all information stored in the wiki (but not some protected information like	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-7fqr-97j7-jgf4, https://github.com/xwiki/xwiki-platform/commit/93b8ec702d7075f0f5794bb05dfb651382596764, https://jira.xwiki.org/browse/XWIKI-21138	A-XWI-XWIK-181223/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password hashes). While there is a right check normally, the right check can be circumvented by explicitly requesting fields from Solr that don't include the data for the right check. This has been fixed in XWiki 15.6RC1, 15.5.1 and 14.10.15 by not listing documents whose rights cannot be checked. No known workarounds are available. **CVE ID : CVE-2023-48241**		
Affected Version(s): From (including) 11.10.1 Up to (excluding) 14.10.15					
Server-Side Request Forgery (SSRF)	20-Nov-2023	8.8	XWiki Platform is a generic wiki platform. The rendered diff in XWiki embeds images to be able to compare the contents and not display a difference for an actually unchanged image. For this, XWiki requests all embedded images on the server side. These requests are also sent for images from other domains and include all cookies that were	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-7rfg-6273-f5wp, https://github.com/xwiki/xwiki-platform/commit/bff0203e739b6e3eb90af5736f04278c73c2a8bb, https://jira.xwiki.org/browse/XWIKI-20818	A-XWI-XWIK-181223/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	sent in the original request to ensure that images with restricted view right can be compared. Starting in version 11.10.1 and prior to versions 14.10.15, 15.5.1, and 15.6, this allows an attacker to steal login and session cookies that allow impersonating the current user who views the diff. The attack can be triggered with an image that references the rendered diff, thus making it easy to trigger. Apart from stealing login cookies, this also allows server-side request forgery (the result of any successful request is returned in the image's source) and viewing protected content as once a resource is cached, it is returned for all users. As only successful requests are cached, the cache will be filled by the first user who is allowed to access the resource. This has been		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched in XWiki 14.10.15, 15.5.1 and 15.6. The rendered diff now only downloads images from trusted domains. Further, cookies are only sent when the image's domain is the same the requested domain. The cache has been changed to be specific for each user. As a workaround, the image embedding feature can be disabled by deleting `xwiki-platform-diff-xml-<version>.jar` in `WEB-INF/lib/`. **CVE ID : CVE-2023-48240**		
Affected Version(s): From (including) 15.0 Up to (excluding) 15.5.1					
Server-Side Request Forgery (SSRF)	20-Nov-2023	8.8	XWiki Platform is a generic wiki platform. The rendered diff in XWiki embeds images to be able to compare the contents and not display a difference for an actually unchanged image. For this, XWiki requests all embedded images on the server side. These requests are	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-7rfg-6273-f5wp, https://github.com/xwiki/xwiki-platform/commit/bff0203e739b6e3eb90af5736f04278c73c2a8bb, https://jira.xwi	A-XWI-XWIK-181223/1054

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
			also sent for images from other domains and include all cookies that were sent in the original request to ensure that images with restricted view right can be compared. Starting in version 11.10.1 and prior to versions 14.10.15, 15.5.1, and 15.6, this allows an attacker to steal login and session cookies that allow impersonating the current user who views the diff. The attack can be triggered with an image that references the rendered diff, thus making it easy to trigger. Apart from stealing login cookies, this also allows server-side request forgery (the result of any successful request is returned in the image's source) and viewing protected content as once a resource is cached, it is returned for all users. As only successful requests are cached, the cache will be filled	ki.org/browse/ XWIKI-20818	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by the first user who is allowed to access the resource. This has been patched in XWiki 14.10.15, 15.5.1 and 15.6. The rendered diff now only downloads images from trusted domains. Further, cookies are only sent when the image's domain is the same the requested domain. The cache has been changed to be specific for each user. As a workaround, the image embedding feature can be disabled by deleting `xwiki-platform-diff-xml-<version>.jar` in `WEB-INF/lib/`. **CVE ID : CVE-2023-48240**		
N/A	20-Nov-2023	7.5	XWiki Platform is a generic wiki platform. Starting in version 6.3-milestone-2 and prior to versions 14.10.15, 15.5.1, and 15.6RC1, the Solr-based search suggestion provider that also duplicates as generic JavaScript	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-7fqr-97j7-jgf4, https://github.com/xwiki/xwiki-platform/commit/93b8ec702d7075f0f5794b	A-XWI-XWIK-181223/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			API for search results in XWiki exposes the content of all documents of all wikis to anybody who has access to it, by default it is public. This exposes all information stored in the wiki (but not some protected information like password hashes). While there is a right check normally, the right check can be circumvented by explicitly requesting fields from Solr that don't include the data for the right check. This has been fixed in XWiki 15.6RC1, 15.5.1 and 14.10.15 by not listing documents whose rights cannot be checked. No known workarounds are available. **CVE ID : CVE-2023-48241**	b05dfb651382596764, https://jira.xwiki.org/browse/XWIKI-21138	
Affected Version(s): From (including) 6.4 Up to (excluding) 14.10.5					
N/A	20-Nov-2023	7.5	XWiki Platform is a generic wiki platform. Starting in version 6.3-milestone-2 and prior to versions 14.10.15, 15.5.1,	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-7fqr-97j7-jgf4,	A-XWI-XWIK-181223/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 15.6RC1, the Solr-based search suggestion provider that also duplicates as generic JavaScript API for search results in XWiki exposes the content of all documents of all wikis to anybody who has access to it, by default it is public. This exposes all information stored in the wiki (but not some protected information like password hashes). While there is a right check normally, the right check can be circumvented by explicitly requesting fields from Solr that don't include the data for the right check. This has been fixed in XWiki 15.6RC1, 15.5.1 and 14.10.15 by not listing documents whose rights cannot be checked. No known workarounds are available. **CVE ID : CVE-2023-48241**	https://github.com/xwiki/xwiki-platform/commit/93b8ec702d7075f0f5794bb05dfb651382596764, https://jira.xwiki.org/browse/XWIKI-21138	
Vendor: yasglobal					
Product: permalinks_customizer					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Nov-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in YAS Global Team Permalinks Customizer plugin <= 2.8.2 versions. **CVE ID : CVE-2023-47773**	N/A	A-YAS-PERM-181223/1057
Vendor: Yoast					
Product: yoast_local_seo					
Affected Version(s): * Up to (including) 14.8					
N/A	18-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Yoast Yoast Local Premium.This issue affects Yoast Local Premium: from n/a through 14.8. **CVE ID : CVE-2023-28780**	N/A	A-YOA-YOAS-181223/1058
Vendor: yoohooplugins					
Product: when_last_login					
Affected Version(s): * Up to (including) 1.2.1					
N/A	22-Nov-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Yoohoo Plugins When Last Login plugin <= 1.2.1 versions.	N/A	A-YOO-WHEN-181223/1059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27461		
Vendor: zlib-ng					
Product: minizip-ng					
Affected Version(s): 4.0.2					
Out-of-bounds Write	22-Nov-2023	8.8	Buffer Overflow vulnerability in zlib-ng minizip-ng v.4.0.2 allows an attacker to execute arbitrary code via a crafted file to the mz_path_has_slash function in the mz_os.c file. **CVE ID : CVE-2023-48107**	https://github.com/zlib-ng/minizip-ng/issues/739	A-ZLI-MINI-181223/1060
Vendor: zorem					
Product: advanced_local_pickup_for_woocommerce					
Affected Version(s): * Up to (including) 1.5.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Nov-2023	7.2	The Advanced Local Pickup for WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the id parameter in versions up to, and including, 1.5.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated	N/A	A-ZOR-ADVA-181223/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers with admin-level privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-2841**		
Vendor: zscaler					
Product: client_connector					
Affected Version(s): * Up to (excluding) 4.2.0.149					
Improper Validation of Integrity Check Value	21-Nov-2023	5.4	An Improper Validation of Integrity Check Value in Zscaler Client Connector on Windows allows an authenticated user to disable ZIA/ZPA by interrupting the service restart from Zscaler Diagnostics. This issue affects Client Connector: before 4.2.0.149. **CVE ID : CVE-2023-28802**	N/A	A-ZSC-CLIE-181223/1062
Vendor: Zulip					
Product: zulip_server					
Affected Version(s): From (including) 1.3.0 Up to (excluding) 7.5					
N/A	16-Nov-2023	4.3	Zulip is an open-source team collaboration tool.	https://github.com/zulip/zulip/security/adv	A-ZUL-ZULI-181223/1063

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
			It was discovered by the Zulip development team that active users who had previously been subscribed to a stream incorrectly continued being able to use the Zulip API to access metadata for that stream. As a result, users who had been removed from a stream, but still had an account in the organization, could still view metadata for that stream (including the stream name, description, settings, and an email address used to send emails into the stream via the incoming email integration). This potentially allowed users to see changes to a stream's metadata after they had lost access to the stream. This vulnerability has been addressed in version 7.5 and all users are advised to upgrade. There are no known workarounds for this issue.	isories/GHSA-c9wc-65fh-9x8p, https://github.com/zulip/zulip/commit/6336322d2f9bbccaacfc80cba83a3c62eefd5737	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47642		
Vendor: Zyxel					
Product: secuextender_ssl_vpn					
Affected Version(s): 4.0.4.0					
N/A	20-Nov-2023	0	The out-of-bounds write vulnerability in the Windows-based SecuExtender SSL VPN Client software version 4.0.4.0 could allow an authenticated local user to gain a privilege escalation by sending a crafted CREATE message. **CVE ID : CVE-2023-5593**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-out-of-bounds-write-vulnerability-in-secuextender-ssl-vpn-client-software	A-ZYX-SECU-181223/1064
Hardware					
Vendor: autelrobotics					
Product: evo_nano_drone					
Affected Version(s): -					
Incorrect Default Permissions	16-Nov-2023	6.5	Insecure permissions in the setNFZEnable function of Autel Robotics EVO Nano drone v1.6.5 allows attackers to breach the geo-fence and fly into no-fly zones. **CVE ID : CVE-2023-47335**	N/A	H-AUT-EVO_-191223/1065
Vendor: Cisco					
Product: ip_dect_110					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	A vulnerability in the web-based management interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid credentials to access the web-based management	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA	H-CIS-IP_D-191223/1066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of the affected device. **CVE ID : CVE-2023-20265**		
Product: ip_dect_210					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	A vulnerability in the web-based management interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA	H-CIS-IP_D-191223/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, the attacker must have valid credentials to access the web-based management interface of the affected device. **CVE ID : CVE-2023-20265**		
Product: unified_ip_phone_6901					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	A vulnerability in the web-based management interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA	H-CIS-UNIF-191223/1068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid credentials to access the web-based management interface of the affected device. **CVE ID : CVE-2023-20265**		
Product: unified_sip_phone_3905					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	A vulnerability in the web-based management interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA	H-CIS-UNIF-191223/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid credentials to access the web-based management interface of the affected device. **CVE ID : CVE-2023-20265**		
Vendor: Dell					
Product: precision_5820					
Affected Version(s): -					
Improper Input Validation	16-Nov-2023	6.7	Dell Precision Tower BIOS contains an Improper Input Validation vulnerability. A locally authenticated malicious user with admin privileges could potentially exploit this vulnerability to perform arbitrary code execution.	https://www.dell.com/support/kbdoc/en-us/000216242/dsa-2023-223-security-update-for-a-dell-precision-tower-bios-vulnerability	H-DEL-PREC-191223/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32469		
Product: precision_7820					
Affected Version(s): -					
Improper Input Validation	16-Nov-2023	6.7	Dell Precision Tower BIOS contains an Improper Input Validation vulnerability. A locally authenticated malicious user with admin privileges could potentially exploit this vulnerability to perform arbitrary code execution. **CVE ID : CVE-2023-32469**	https://www.dell.com/support/kbdoc/en-us/000216242/dsa-2023-223-security-update-for-a-dell-precision-tower-bios-vulnerability	H-DEL-PREC-191223/1071
Product: precision_7920					
Affected Version(s): -					
Improper Input Validation	16-Nov-2023	6.7	Dell Precision Tower BIOS contains an Improper Input Validation vulnerability. A locally authenticated malicious user with admin privileges could potentially exploit this vulnerability to	https://www.dell.com/support/kbdoc/en-us/000216242/dsa-2023-223-security-update-for-a-dell-precision-tower-bios-vulnerability	H-DEL-PREC-191223/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform arbitrary code execution. **CVE ID : CVE-2023-32469**		
Vendor: Draytek					
Product: vigor2960					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-2023	8.1	Draytek Vigor2960 v1.5.1.4 and v1.5.1.5 are vulnerable to directory traversal via the mainfunction.cgi dumpSyslog 'option' parameter allowing an authenticated attacker with access to the web management interface to delete arbitrary files. Vigor2960 is no longer supported. **CVE ID : CVE-2023-6265**	N/A	H-DRA-VIGO-191223/1073
Vendor: elecom					
Product: wrc-x3000gs2-b					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	16-Nov-2023	8	OS command injection vulnerability in WRC-X3000GS2-W v1.05 and earlier, WRC-X3000GS2-B v1.05 and earlier, and WRC-	https://www.elecom.co.jp/news/security/20231114-01/	H-ELE-WRC--191223/1074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			X3000GS2A-B v1.05 and earlier allows a network-adjacent authenticated user to execute an arbitrary OS command by sending a specially crafted request. **CVE ID : CVE-2023-43752**		
Product: wrc-x3000gs2-w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Nov-2023	8	OS command injection vulnerability in WRC-X3000GS2-W v1.05 and earlier, WRC-X3000GS2-B v1.05 and earlier, and WRC-X3000GS2A-B v1.05 and earlier allows a network-adjacent authenticated user to execute an arbitrary OS command by sending a specially crafted request. **CVE ID : CVE-2023-43752**	https://www.elecom.co.jp/news/security/20231114-01/	H-ELE-WRC--191223/1075
Product: wrc-x3000gs2a-b					
Affected Version(s): -					
Improper Neutralization of Special Elements	16-Nov-2023	8	OS command injection vulnerability in WRC-X3000GS2-W v1.05 and earlier,	https://www.elecom.co.jp/news/security/20231114-01/	H-ELE-WRC--191223/1076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			WRC-X3000GS2-B v1.05 and earlier, and WRC-X3000GS2A-B v1.05 and earlier allows a network-adjacent authenticated user to execute an arbitrary OS command by sending a specially crafted request. **CVE ID : CVE-2023-43752**		
Vendor: inea					
Product: me_rtu					
Affected Version(s): -					
Improper Authentication	20-Nov-2023	9.8	Versions of INEA ME RTU firmware 3.36b and prior do not require authentication to the "root" account on the host system of the device. This could allow an attacker to obtain admin-level access to the host system. **CVE ID : CVE-2023-29155**	N/A	H-INE-ME_R-191223/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Nov-2023	9.8	Versions of INEA ME RTU firmware 3.36b and prior are vulnerable to operating system (OS) command injection, which could allow remote code execution. **CVE ID : CVE-2023-35762**	N/A	H-INE-ME_R-191223/1078
Vendor: neutron					
Product: ipc2224-sr3-npf-36					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-IPC2-191223/1079
Product: ipc2624-sr3-npf-36					
Affected Version(s): -					
Improper Limitation of a	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in	N/A	H-NEU-IPC2-191223/1080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**		
Product: neu-ipb210-28					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NEU--191223/1081
Product: neu-ipb410-28					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1.	N/A	H-NEU-NEU--191223/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6118		
Product: neu-ipbm211					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NEU--191223/1083
Product: neu-ipbm411					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NEU--191223/1084
Product: neu-ipd220-28					
Affected Version(s): -					
Improper Limitation of a Pathname to a	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute	N/A	H-NEU-NEU--191223/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**		
Product: neu-ipdm221					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NEU--191223/1086
Product: neu-ipdm421					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NEU--191223/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ntl-bc-01w					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NTL--191223/1088
Product: ntl-bc-03-snm					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NTL--191223/1089
Product: ntl-bc-03-snp					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP	N/A	H-NEU-NTL--191223/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**		
Product: ntl-bc01-m					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NTL--191223/1091
Product: ntl-ip05-3mp					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NTL--191223/1092
Product: ntl-pt-06wod-3mp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NTL--191223/1093
Product: ntl-pt-09-wos-3mp					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	H-NEU-NTL--191223/1094
Product: ntl-pt-10-4gwos-3mp					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1.	N/A	H-NEU-NTL--191223/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6118		
Vendor: redlioncontrols					
Product: st-ipm-6350					
Affected Version(s): -					
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-40151**	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	H-RED-ST-I-191223/1096

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
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-42770**	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	H-RED-ST-I-191223/1097
Product: st-ipm-8460					
Affected Version(s): -					
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	H-RED-ST-I-191223/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-40151**		
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-42770**	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	H-RED-ST-I-191223/1099
Product: vt-ipm2m-113-d					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-40151**	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	H-RED-VT-I-191223/1100
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-	H-RED-VT-I-191223/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-42770**	Remote-Code-Execution	
Product: vt-ipm2m-213-d					
Affected Version(s): -					
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge.	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	H-RED-VT-I-191223/1102

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-2023-40151		
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-42770**	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	H-RED-VT-I-191223/1103
Product: vt-mipm-135-d					
Affected Version(s): -					
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges.	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-	H-RED-VT-M-191223/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-40151**	Remote-Code-Execution	
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge.	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	H-RED-VT-M-191223/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42770		
Product: vt-mipm-245-d					
Affected Version(s): -					
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-40151**	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	H-RED-VT-M-191223/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-42770**	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	H-RED-VT-M-191223/1107
Vendor: Tenda					
Product: ac10					
Affected Version(s): 4.0					
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the list parameter in the function sub_49E098. **CVE ID : CVE-2023-45479**	N/A	H-TEN-AC10-191223/1108
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was	N/A	H-TEN-AC10-191223/1109

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
			discovered to contain a stack overflow via the src parameter in the function sub_47D878. **CVE ID : CVE-2023-45480**		
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the firewallEn parameter in the function SetFirewallCfg. **CVE ID : CVE-2023-45481**	N/A	H-TEN-AC10-191223/1110
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the urls parameter in the function get_parentControl_list_Info. **CVE ID : CVE-2023-45482**	N/A	H-TEN-AC10-191223/1111
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the time parameter in	N/A	H-TEN-AC10-191223/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the function compare_parentcontrol_time. **CVE ID : CVE-2023-45483**		
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the shareSpeed parameter in the function fromSetWifiGuestBasic. **CVE ID : CVE-2023-45484**	N/A	H-TEN-AC10-191223/1113
Product: ac18					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda Ac19 v.1.0, AC18, AC9 v.1.0, AC6 v.2.0 and v.1.0 allows a remote attacker to execute arbitrary code via the formSetCfm function in bin/httpd. **CVE ID : CVE-2023-38823**	N/A	H-TEN-AC18-191223/1114
Product: ac19					
Affected Version(s): 1.0					
Buffer Copy without Checking Size of	20-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda Ac19 v.1.0, AC18, AC9 v.1.0, AC6 v.2.0 and v.1.0	N/A	H-TEN-AC19-191223/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			allows a remote attacker to execute arbitrary code via the formSetCfm function in bin/httpd. **CVE ID : CVE-2023-38823**		
Product: ac6					
Affected Version(s): 1.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda Ac19 v.1.0, AC18, AC9 v.1.0, AC6 v.2.0 and v.1.0 allows a remote attacker to execute arbitrary code via the formSetCfm function in bin/httpd. **CVE ID : CVE-2023-38823**	N/A	H-TEN-AC6-191223/1116
Affected Version(s): 2.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda Ac19 v.1.0, AC18, AC9 v.1.0, AC6 v.2.0 and v.1.0 allows a remote attacker to execute arbitrary code via the formSetCfm function in bin/httpd. **CVE ID : CVE-2023-38823**	N/A	H-TEN-AC6-191223/1117
Product: ac9					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda Ac19 v.1.0, AC18, AC9 v.1.0, AC6 v.2.0 and v.1.0 allows a remote attacker to execute arbitrary code via the formSetCfm function in bin/httpd. **CVE ID : CVE-2023-38823**	N/A	H-TEN-AC9-191223/1118
Product: ax1803					
Affected Version(s): -					
Out-of-bounds Write	27-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the wpapsk_crypto parameter in the function fromSetWirelessRepeat. **CVE ID : CVE-2023-49043**	N/A	H-TEN-AX18-191223/1119
Out-of-bounds Write	27-Nov-2023	9.8	Stack Overflow vulnerability in Tenda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the ssid parameter in the function form_fast_setting_wifi_set.	N/A	H-TEN-AX18-191223/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49044		
Out-of-bounds Write	27-Nov-2023	9.8	Stack Overflow vulnerability in Tenda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the devName parameter in the function formAddMacfilterRule. **CVE ID : CVE-2023-49046**	N/A	H-TEN-AX18-191223/1121
Out-of-bounds Write	20-Nov-2023	7.5	Tenda AX1803 v1.0.0.1 was discovered to contain a heap overflow via the deviceId parameter in the function saveParentControlInfo . This vulnerability allows attackers to cause a Denial of Service (DoS) attack **CVE ID : CVE-2023-48109**	N/A	H-TEN-AX18-191223/1122
Out-of-bounds Write	20-Nov-2023	7.5	Tenda AX1803 v1.0.0.1 was discovered to contain a heap overflow via the urls parameter in the function saveParentControlInfo . This vulnerability allows attackers to cause a	N/A	H-TEN-AX18-191223/1123

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
			Denial of Service (DoS) attack **CVE ID : CVE-2023-48110**		
Out-of-bounds Write	20-Nov-2023	7.5	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow via the time parameter in the function saveParentControlInfo . This vulnerability allows attackers to cause a Denial of Service (DoS) attack **CVE ID : CVE-2023-48111**	N/A	H-TEN-AX18-191223/1124
Vendor: totolink					
Product: a3700r					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	20-Nov-2023	7.8	An issue in TOTOlink A3700R v.9.1.2u.6134_B20201202 allows a local attacker to execute arbitrary code via the setTracerouteCfg function. **CVE ID : CVE-2023-48192**	N/A	H-TOT-A370-191223/1125
Vendor: unitree					
Product: a1					
Affected Version(s): 1.16					
Missing Authentication for	22-Nov-2023	7.5	Lack of authentication vulnerability. An unauthenticated	https://www.incibe.es/en/incibe-cert/notices/av	H-UNI-A1-191223/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			local user is able to see through the cameras using the web server due to the lack of any form of authentication. **CVE ID : CVE-2023-3104**	iso/multiple-vulnerabilities-unitree-robotics-a1	
N/A	22-Nov-2023	5.9	Authentication bypass vulnerability, the exploitation of which could allow a local attacker to perform a Man-in-the-Middle (MITM) attack on the robot's camera video stream. In addition, if a MITM attack is carried out, it is possible to consume the robot's resources, which could lead to a denial-of-service (DOS) condition. **CVE ID : CVE-2023-3103**	https://www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-unitree-robotics-a1	H-UNI-A1-191223/1127
Vendor: Wago					
Product: 0852-0602					
Affected Version(s): -					
N/A	21-Nov-2023	0	A vulnerability in the web-based management allows an unauthenticated remote attacker to inject arbitrary system commands and gain full system control. Those	N/A	H-WAG-0852-191223/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands are executed with root privileges. The vulnerability is located in the user request handling of the web-based management. **CVE ID : CVE-2023-4149**		
Product: 0852-0603					
Affected Version(s): -					
N/A	21-Nov-2023	0	A vulnerability in the web-based management allows an unauthenticated remote attacker to inject arbitrary system commands and gain full system control. Those commands are executed with root privileges. The vulnerability is located in the user request handling of the web-based management. **CVE ID : CVE-2023-4149**	N/A	H-WAG-0852-191223/1129
Product: 0852-1605					
Affected Version(s): -					
N/A	21-Nov-2023	0	A vulnerability in the web-based management allows an unauthenticated remote attacker to inject arbitrary	N/A	H-WAG-0852-191223/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system commands and gain full system control. Those commands are executed with root privileges. The vulnerability is located in the user request handling of the web-based management. **CVE ID : CVE-2023-4149**		
Product: compact_controller_100					
Affected Version(s): -					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	H-WAG-COMP-191223/1131
Product: edge_controller					
Affected Version(s): -					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to	N/A	H-WAG-EDGE-191223/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate non-root privileges. **CVE ID : CVE-2023-3379**		
Product: pfc100					
Affected Version(s): -					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	H-WAG-PFC1-191223/1133
Product: pfc200					
Affected Version(s): -					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	H-WAG-PFC2-191223/1134
Product: touch_panel_600_advanced					
Affected Version(s): -					
N/A	20-Nov-2023	0	Wago web-based management of	N/A	H-WAG-TOUC-191223/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**		
Product: touch_panel_600_marine					
Affected Version(s): -					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	H-WAG-TOUC-191223/1136
Product: touch_panel_600_standard					
Affected Version(s): -					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to	N/A	H-WAG-TOUC-191223/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate non-root privileges. **CVE ID : CVE-2023-3379**		
Operating System					
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Out-of-bounds Read	16-Nov-2023	7.8	Adobe InCopy versions 18.5 (and earlier) and 17.4.2 (and earlier) are affected by 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-2023-26368**	https://helpx.adobe.com/security/products/incopy/apsb23-60.html	O-APP-MACO-191223/1138
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an out-of-	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	O-APP-MACO-191223/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47043**		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47046**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-APP-MACO-191223/1140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-47047**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-APP-MACO-191223/1141
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-APP-MACO-191223/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-47048**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47049**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-APP-MACO-191223/1143
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (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	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-APP-MACO-191223/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-44330**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44338**	N/A	O-APP-MACO-191223/1145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47050**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-APP-MACO-191223/1146
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-APP-MACO-191223/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-47051**		
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47066**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-APP-MACO-191223/1148
Use After Free	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-APP-MACO-191223/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47055**		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44336**	N/A	O-APP-MACO-191223/1150
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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	N/A	O-APP-MACO-191223/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-44337**		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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-2023-47056**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-APP-MACO-191223/1152
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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.	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-APP-MACO-191223/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47057**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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-2023-47058**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-APP-MACO-191223/1154
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-APP-MACO-191223/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47059**		
Out-of-bounds Write	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47073**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-APP-MACO-191223/1156
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-APP-MACO-191223/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47067**		
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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.	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-APP-MACO-191223/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47068		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44359**	N/A	O-APP-MACO-191223/1159
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-APP-MACO-191223/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47069**		
Out-of-bounds Write	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47070**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-APP-MACO-191223/1161
Access of Uninitialized Pointer	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an Access of Uninitialized Pointer 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	N/A	O-APP-MACO-191223/1162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-44365**		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44366**	N/A	O-APP-MACO-191223/1163
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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	N/A	O-APP-MACO-191223/1164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-44367**		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44371**	N/A	O-APP-MACO-191223/1165
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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.	N/A	O-APP-MACO-191223/1166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-44372		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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-2023-47040**	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	O-APP-MACO-191223/1167
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	O-APP-MACO-191223/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47041**		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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-2023-47042**	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	O-APP-MACO-191223/1169
Out-of-bounds Read	17-Nov-2023	5.5	Adobe Animate versions 23.0.2 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/animate/apsb23-61.html	O-APP-MACO-191223/1170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-44325**		
Out-of-bounds Read	17-Nov-2023	5.5	Adobe Dimension versions 3.4.9 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44326**	https://helpx.adobe.com/security/products/dimension/apsb23-62.html	O-APP-MACO-191223/1171
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	O-APP-MACO-191223/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44327**		
Use After Free	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44328**	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	O-APP-MACO-191223/1173
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	O-APP-MACO-191223/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44329**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44332**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-APP-MACO-191223/1175
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-APP-MACO-191223/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44333**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44334**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-APP-MACO-191223/1177
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-APP-MACO-191223/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44335**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44331**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-APP-MACO-191223/1179
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to	N/A	O-APP-MACO-191223/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44340**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44348**	N/A	O-APP-MACO-191223/1181
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and	N/A	O-APP-MACO-191223/1182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44356**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44357**	N/A	O-APP-MACO-191223/1183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44358**	N/A	O-APP-MACO-191223/1184
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	N/A	O-APP-MACO-191223/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44360**		
Use After Free	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44361**	N/A	O-APP-MACO-191223/1186
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-APP-MACO-191223/1187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47052**		
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47053**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-APP-MACO-191223/1188
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory.	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	O-APP-MACO-191223/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47044**		
Out-of-bounds Read	17-Nov-2023	5.5	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47071**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-APP-MACO-191223/1190
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-APP-MACO-191223/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47054**		
Out-of-bounds Read	16-Nov-2023	5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44339**	N/A	O-APP-MACO-191223/1192
Access of Uninitialized Pointer	16-Nov-2023	3.3	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier)	https://helpx.adobe.com/security/products/	O-APP-MACO-191223/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47060**	premiere_pro/apsb23-65.html	
Access of Uninitialized Pointer	17-Nov-2023	3.3	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-APP-MACO-191223/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47072		
Vendor: autelrobotics					
Product: evo_nano_drone_firmware					
Affected Version(s): 1.6.5					
Incorrect Default Permissions	16-Nov-2023	6.5	Insecure permissions in the setNFZEnable function of Autel Robotics EVO Nano drone v1.6.5 allows attackers to breach the geo-fence and fly into no-fly zones. **CVE ID : CVE-2023-47335**	N/A	O-AUT-EVO_-191223/1195
Vendor: Axis					
Product: axis_os					
Affected Version(s): * Up to (excluding) 11.7.57					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	7.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API manageoverlayimage.cgi was vulnerable to path traversal attacks that allows for file/folder deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. The	https://www.axis.com/dam/public/2a/82/12/cve-2023-21417-en-US-417791.pdf	O-AXI-AXIS-191223/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact of exploiting this vulnerability is lower with operator service accounts and limited to non-system files compared to administrator-privileges. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21417**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	7.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API irissetup.cgi was vulnerable to path traversal attacks that allows for file deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. The	https://www.axis.com/dam/public/49/93/55/cve-2023-21418-en-US-417792.pdf	O-AXI-AXIS-191223/1197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact of exploiting this vulnerability is lower with operator service accounts and limited to non-system files compared to administrator-privileges. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21418**		
N/A	21-Nov-2023	6.5	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API dynamicoverlay.cgi was vulnerable to a Denial-of-Service attack allowing for an attacker to block access to the overlay configuration page in the web interface of the Axis device. This flaw can only be exploited after authenticating with	https://www.axis.com/dam/public/35/2a/a6/cve-2023-21416-en-US-417790.pdf	O-AXI-AXIS-191223/1198

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
			an operator- or administrator-privileged service account however the impact is equal. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21416**		
Affected Version(s): * Up to (excluding) 6.50.5.15					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	7.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API irissetup.cgi was vulnerable to path traversal attacks that allows for file deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. The impact of exploiting this vulnerability is lower with operator service accounts and limited to non-	https://www.axis.com/dam/public/49/93/55/cve-2023-21418-en-US-417792.pdf	O-AXI-AXIS-191223/1199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system files compared to administrator-privileges. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21418**		
Product: axis_os_2018					
Affected Version(s): * Up to (excluding) 8.40.35					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	7.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API irissetup.cgi was vulnerable to path traversal attacks that allows for file deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. The impact of exploiting this vulnerability is lower with operator service	https://www.axis.com/dam/public/49/93/55/cve-2023-21418-en-US-417792.pdf	O-AXI-AXIS-191223/1200

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
			accounts and limited to non-system files compared to administrator-privileges. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21418**		
Product: axis_os_2020					
Affected Version(s): * Up to (excluding) 9.80.49					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	7.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API manageoverlayimage.cgi was vulnerable to path traversal attacks that allows for file/folder deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service	https://www.axis.com/dam/public/2a/82/12/cve-2023-21417-en-US-417791.pdf	O-AXI-AXIS-191223/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account. The impact of exploiting this vulnerability is lower with operator service accounts and limited to non-system files compared to administrator-privileges. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21417**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	7.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API irissetup.cgi was vulnerable to path traversal attacks that allows for file deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service	https://www.axis.com/dam/public/49/93/55/cve-2023-21418-en-US-417792.pdf	O-AXI-AXIS-191223/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account. The impact of exploiting this vulnerability is lower with operator service accounts and limited to non-system files compared to administrator-privileges. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21418**		
Product: axis_os_2022					
Affected Version(s): * Up to (excluding) 10.12.208					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	7.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API manageoverlayimage.cgi was vulnerable to path traversal attacks that allows for file/folder deletion. This flaw can only	https://www.axis.com/dam/public/2a/82/12/cve-2023-21417-en-US-417791.pdf	O-AXI-AXIS-191223/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be exploited after authenticating with an operator- or administrator-privileged service account. The impact of exploiting this vulnerability is lower with operator service accounts and limited to non-system files compared to administrator-privileges. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21417**		
Affected Version(s): * Up to (excluding) 10.12.213					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	7.1	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API irissetup.cgi was vulnerable to path traversal attacks that allows for file	https://www.axis.com/dam/public/49/93/55/cve-2023-21418-en-US-417792.pdf	O-AXI-AXIS-191223/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deletion. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. The impact of exploiting this vulnerability is lower with operator service accounts and limited to non-system files compared to administrator-privileges. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21418**		
N/A	21-Nov-2023	6.5	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API dynamicoverlay.cgi was vulnerable to a Denial-of-Service attack allowing for an attacker to block	https://www.axis.com/dam/public/35/2a/a6/cve-2023-21416-en-US-417790.pdf	O-AXI-AXIS-191223/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to the overlay configuration page in the web interface of the Axis device. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account however the impact is equal. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution. **CVE ID : CVE-2023-21416**		
Vendor: Cisco					
Product: ip_dect_110_firmware					
Affected Version(s): * Up to (excluding) 5.1.2sr1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	A vulnerability in the web-based management interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA	O-CIS-IP_D-191223/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid credentials to access the web-based management interface of the affected device. **CVE ID : CVE-2023-20265**		
Product: ip_dect_210_firmware					
Affected Version(s): * Up to (excluding) 5.1.2sr1					
Improper Neutralization of Input During Web Page Generation	21-Nov-2023	5.4	A vulnerability in the web-based management interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-IP_D-191223/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid credentials to access the web-based management interface of the affected device. **CVE ID : CVE-2023-20265**	uipphone-xss-NcmUykqA	
Product: unified_ip_phone_6901_firmware					
Affected Version(s): From (including) 9.0 Up to (excluding) 9.3\\(1\\)sr3					
Improper Neutralization of	21-Nov-2023	5.4	A vulnerability in the web-based management	https://sec.cloudapps.cisco.com/security/cen	O-CIS-UNIF-191223/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid credentials to access the web-based management interface of the affected device. **CVE ID : CVE-2023-20265**	ter/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: unified_sip_phone_3905_firmware					
Affected Version(s): From (including) 9.0 Up to (excluding) 9.4\\(1\\)sr4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Nov-2023	5.4	A vulnerability in the web-based management interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid credentials to access the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uipphone-xss-NcmUykqA	O-CIS-UNIF-191223/1209

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
			based management interface of the affected device. **CVE ID : CVE-2023-20265**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Use After Free	21-Nov-2023	8.8	Ownership mismanagement led to a use-after-free in ReadableByteStreams This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6207**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1210
N/A	21-Nov-2023	8.8	When using X11, text selected by the page using the Selection API was erroneously copied into the primary selection, a temporary storage not unlike the clipboard. *This bug only affects Firefox on X11. Other systems are unaffected.* This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.5. **CVE ID : CVE-2023-6208**		
Out-of-bounds Write	21-Nov-2023	8.8	Memory safety bugs present in Firefox 119, Firefox ESR 115.4, and Thunderbird 115.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6212**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1212
Out-of-bounds Read	21-Nov-2023	6.5	On some systems—depending on the graphics settings and drivers—it was possible to force an out-of-bounds read and leak memory data into the images created on the canvas element. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5.	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1213

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-2023-6204		
Use After Free	21-Nov-2023	6.5	It was possible to cause the use of a MessagePort after it had already been freed, which could potentially have led to an exploitable crash. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6205**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1214
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	6.5	Relative URLs starting with three slashes were incorrectly parsed, and a path-traversal "/../" part in the path could be used to override the specified host. This could contribute to security problems in web sites. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6209**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1215
Improper Restriction of	21-Nov-2023	5.4	The black fade animation when exiting fullscreen is	https://www.mozilla.org/security/advisorie	O-DEB-DEBI-191223/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Rendered UI Layers or Frames			roughly the length of the anti-clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6206**	s/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	
Affected Version(s): 11.0					
Use After Free	21-Nov-2023	8.8	Ownership mismanagement led to a use-after-free in ReadableByteStreams This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6207**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1217
N/A	21-Nov-2023	8.8	When using X11, text selected by the page using the Selection API was erroneously copied into the primary selection, a	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/sec	O-DEB-DEBI-191223/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			temporary storage not unlike the clipboard. *This bug only affects Firefox on X11. Other systems are unaffected.* This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6208**	urity/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	
Out-of-bounds Write	21-Nov-2023	8.8	Memory safety bugs present in Firefox 119, Firefox ESR 115.4, and Thunderbird 115.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6212**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1219
Out-of-bounds Read	21-Nov-2023	6.5	On some systems—depending on the graphics settings and drivers—it was possible to force an	https://www.mozilla.org/security/advisories/mfsa2023-49/,	O-DEB-DEBI-191223/1220

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
			out-of-bounds read and leak memory data into the images created on the canvas element. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6204**	https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	
Use After Free	21-Nov-2023	6.5	It was possible to cause the use of a MessagePort after it had already been freed, which could potentially have led to an exploitable crash. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6205**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1221
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	6.5	Relative URLs starting with three slashes were incorrectly parsed, and a path-traversal "/../" part in the path could be used to override the specified host. This could contribute to security problems in web sites. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisorie	O-DEB-DEBI-191223/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6209**	s/mfsa2023-52/	
Improper Restriction of Rendered UI Layers or Frames	21-Nov-2023	5.4	The black fade animation when exiting fullscreen is roughly the length of the anti-clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6206**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1223
Affected Version(s): 12.0					
Use After Free	21-Nov-2023	8.8	Ownership mismanagement led to a use-after-free in ReadableByteStreams This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.	O-DEB-DEBI-191223/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.5. **CVE ID : CVE-2023-6207**	mozilla.org/security/advisories/mfsa2023-52/	
N/A	21-Nov-2023	8.8	When using X11, text selected by the page using the Selection API was erroneously copied into the primary selection, a temporary storage not unlike the clipboard. *This bug only affects Firefox on X11. Other systems are unaffected.* This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6208**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1225
Out-of-bounds Write	21-Nov-2023	8.8	Memory safety bugs present in Firefox 119, Firefox ESR 115.4, and Thunderbird 115.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 120,	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6212**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Nov-2023	6.5	SSH dissector crash in Wireshark 4.0.0 to 4.0.10 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-6174**	https://www.wireshark.org/security/wnpa-sec-2023-28.html, https://gitlab.com/wireshark/wireshark/-/issues/19369	O-DEB-DEBI-191223/1227
Out-of-bounds Read	21-Nov-2023	6.5	On some systems—depending on the graphics settings and drivers—it was possible to force an out-of-bounds read and leak memory data into the images created on the canvas element. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6204**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1228
Use After Free	21-Nov-2023	6.5	It was possible to cause the use of a MessagePort after it had already been freed, which could	https://www.mozilla.org/security/advisories/mfsa2023-49/,	O-DEB-DEBI-191223/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially have led to an exploitable crash. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6205**	https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Nov-2023	6.5	Relative URLs starting with three slashes were incorrectly parsed, and a path-traversal "/../" part in the path could be used to override the specified host. This could contribute to security problems in web sites. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6209**	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.mozilla.org/security/advisories/mfsa2023-52/	O-DEB-DEBI-191223/1230
Improper Restriction of Rendered UI Layers or Frames	21-Nov-2023	5.4	The black fade animation when exiting fullscreen is roughly the length of the anti-clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring	https://www.mozilla.org/security/advisories/mfsa2023-49/, https://www.mozilla.org/security/advisories/mfsa2023-50/, https://www.	O-DEB-DEBI-191223/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			them to click where the permission grant button would be about to appear. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5. **CVE ID : CVE-2023-6206**	mozilla.org/security/advisories/mfsa2023-52/	
Vendor: Dell					
Product: os_recovery_tool					
Affected Version(s): 2.2.4013					
N/A	23-Nov-2023	7.8	Dell OS Recovery Tool, versions 2.2.4013, 2.3.7012.0, and 2.3.7515.0 contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability, leading to the elevation of privilege on the system. **CVE ID : CVE-2023-39253**	https://www.dell.com/support/kbdoc/en-us/000217699/dsa-2023-336-security-update-for-a-dell-os-recovery-tool-vulnerability	O-DEL-OS_R-191223/1232
N/A	16-Nov-2023	7.8	Dell OS Recovery Tool, versions	https://www.dell.com/support/kbdoc/en-us/000217078	O-DEL-OS_R-191223/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.2.4013, 2.3.7012.0, and 2.3.7515.0 contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability, leading to the elevation of privilege on the system. **CVE ID : CVE-2023-39259**	/dsa-2023-319dsa-2023-319	
Affected Version(s): 2.3.7012.0					
N/A	23-Nov-2023	7.8	Dell OS Recovery Tool, versions 2.2.4013, 2.3.7012.0, and 2.3.7515.0 contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability, leading to the elevation of privilege on the system.	https://www.dell.com/support/kbdoc/en-us/000217699/dsa-2023-336-security-update-for-a-dell-os-recovery-tool-vulnerability	O-DEL-OS_R-191223/1234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-39253		
N/A	16-Nov-2023	7.8	Dell OS Recovery Tool, versions 2.2.4013, 2.3.7012.0, and 2.3.7515.0 contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability, leading to the elevation of privilege on the system. **CVE ID : CVE-2023-39259**	https://www.dell.com/support/kbdoc/en-us/000217078/dsa-2023-319dsa-2023-319	O-DEL-OS_R-191223/1235
Affected Version(s): 2.3.7515.0					
N/A	23-Nov-2023	7.8	Dell OS Recovery Tool, versions 2.2.4013, 2.3.7012.0, and 2.3.7515.0 contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability, leading to the elevation of	https://www.dell.com/support/kbdoc/en-us/000217699/dsa-2023-336-security-update-for-a-dell-os-recovery-tool-vulnerability	O-DEL-OS_R-191223/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege on the system. **CVE ID : CVE-2023-39253**		
N/A	16-Nov-2023	7.8	Dell OS Recovery Tool, versions 2.2.4013, 2.3.7012.0, and 2.3.7515.0 contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability, leading to the elevation of privilege on the system. **CVE ID : CVE-2023-39259**	https://www.dell.com/support/kbdoc/en-us/000217078/dsa-2023-319dsa-2023-319	O-DEL-OS_R-191223/1237
Product: precision_5820_firmware					
Affected Version(s): * Up to (excluding) 2.32.0					
Improper Input Validation	16-Nov-2023	6.7	Dell Precision Tower BIOS contains an Improper Input Validation vulnerability. A locally authenticated malicious user with	https://www.dell.com/support/kbdoc/en-us/000216242/dsa-2023-223-security-update-for-a-dell-precision-tower-bios-vulnerability	O-DEL-PREC-191223/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin privileges could potentially exploit this vulnerability to perform arbitrary code execution. **CVE ID : CVE-2023-32469**		
Product: precision_7820_firmware					
Affected Version(s): * Up to (excluding) 2.36.0					
Improper Input Validation	16-Nov-2023	6.7	Dell Precision Tower BIOS contains an Improper Input Validation vulnerability. A locally authenticated malicious user with admin privileges could potentially exploit this vulnerability to perform arbitrary code execution. **CVE ID : CVE-2023-32469**	https://www.dell.com/support/kbdoc/en-us/000216242/dsa-2023-223-security-update-for-a-dell-precision-tower-bios-vulnerability	O-DEL-PREC-191223/1239
Product: precision_7920_firmware					
Affected Version(s): * Up to (excluding) 2.36.0					
Improper Input Validation	16-Nov-2023	6.7	Dell Precision Tower BIOS contains an Improper Input	https://www.dell.com/support/kbdoc/en-us/000216242/dsa-2023-223-security-	O-DEL-PREC-191223/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Validation vulnerability. A locally authenticated malicious user with admin privileges could potentially exploit this vulnerability to perform arbitrary code execution. **CVE ID : CVE-2023-32469**	update-for-a-dell-precision-tower-bios-vulnerability	
Vendor: Draytek					
Product: vigor2960_firmware					
Affected Version(s): 1.5.1.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-2023	8.1	Draytek Vigor2960 v1.5.1.4 and v1.5.1.5 are vulnerable to directory traversal via the mainfunction.cgi dumpSyslog 'option' parameter allowing an authenticated attacker with access to the web management interface to delete arbitrary files. Vigor2960 is no longer supported. **CVE ID : CVE-2023-6265**	N/A	O-DRA-VIGO-191223/1241
Affected Version(s): 1.5.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Nov-2023	8.1	Draytek Vigor2960 v1.5.1.4 and v1.5.1.5 are vulnerable to directory traversal via the mainfunction.cgi dumpSyslog 'option' parameter allowing an authenticated attacker with access to the web management interface to delete arbitrary files. Vigor2960 is no longer supported. **CVE ID : CVE-2023-6265**	N/A	O-DRA-VIGO-191223/1242
Vendor: elecom					
Product: wrc-x3000gs2-b_firmware					
Affected Version(s): * Up to (including) 1.05					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Nov-2023	8	OS command injection vulnerability in WRC-X3000GS2-W v1.05 and earlier, WRC-X3000GS2-B v1.05 and earlier, and WRC-X3000GS2A-B v1.05 and earlier allows a network-adjacent authenticated user to execute an arbitrary OS command by sending a specially crafted request.	https://www.elecom.co.jp/news/security/20231114-01/	O-ELE-WRC--191223/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-43752		
Product: wrc-x3000gs2-w_firmware					
Affected Version(s): * Up to (including) 1.05					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Nov-2023	8	OS command injection vulnerability in WRC-X3000GS2-W v1.05 and earlier, WRC-X3000GS2-B v1.05 and earlier, and WRC-X3000GS2A-B v1.05 and earlier allows a network-adjacent authenticated user to execute an arbitrary OS command by sending a specially crafted request. **CVE ID : CVE-2023-43752**	https://www.elecom.co.jp/news/security/20231114-01/	O-ELE-WRC--191223/1244
Product: wrc-x3000gs2a-b_firmware					
Affected Version(s): * Up to (including) 1.05					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Nov-2023	8	OS command injection vulnerability in WRC-X3000GS2-W v1.05 and earlier, WRC-X3000GS2-B v1.05 and earlier, and WRC-X3000GS2A-B v1.05 and earlier allows a network-adjacent authenticated user to execute an arbitrary OS command by	https://www.elecom.co.jp/news/security/20231114-01/	O-ELE-WRC--191223/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a specially crafted request. **CVE ID : CVE-2023-43752**		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 38					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Nov-2023	7.8	A buffer overflow vulnerability was found in the NVM Express (NVMe) driver in the Linux kernel. An unprivileged user could specify a small meta buffer and let the device perform larger Direct Memory Access (DMA) into the same buffer, overwriting unrelated kernel memory, causing random kernel crashes and memory corruption. **CVE ID : CVE-2023-6238**	N/A	O-FED-FEDO-191223/1246
Uncontrolled Resource Consumption	24-Nov-2023	6.5	An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow a remote attacker to cause a denial of service via a craft input with size smaller than 379 KB.	https://bugzilla.redhat.com/show_bug.cgi?id=2251311, https://gitlab.com/libtiff/libtiff/-/issues/614, https://gitlab.com/libtiff/libtiff/-	O-FED-FEDO-191223/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6277	/merge_requests/545	
Affected Version(s): 39					
NULL Pointer Dereference	23-Nov-2023	7.8	A null pointer dereference flaw was found in the nft_inner.c functionality of netfilter in the Linux kernel. This issue could allow a local user to crash the system or escalate their privileges on the system. **CVE ID : CVE-2023-5972**	https://bugzilla.redhat.com/show_bug.cgi?id=2248189, https://github.com/torvalds/linux/commit/505ce0630ad5d31185695f8a29dde8d29f28faa7, https://github.com/torvalds/linux/commit/52177bbf19e6e9398375a148d2e13ed492b40b80	O-FED-FEDO-191223/1248
Improper Handling of Exceptional Conditions	16-Nov-2023	4.3	Vim is an open source command line text editor. A floating point exception may occur when calculating the line offset for overlong lines and smooth scrolling is enabled and the cpo-settings include the 'n' flag. This may happen when a window border is present and when the wrapped line continues on the next physical line directly in the window border because the 'cpo'	https://github.com/vim/vim/security/advisories/GHSA-f6cx-x634-hqpw, https://github.com/vim/vim/commit/cb0b99f0672d8446585d26e998343dceca17d1ce	O-FED-FEDO-191223/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			setting includes the 'n' flag. Only users with non-default settings are affected and the exception should only result in a crash. This issue has been addressed in commit `cb0b99f0` which has been included in release version 9.0.2107. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48232**		
Integer Overflow or Wraparound	16-Nov-2023	4.3	Vim is an open source command line text editor. If the count after the :s command is larger than what fits into a (signed) long variable, abort with e_value_too_large. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `ac6378773` which has been included in release version	https://github.com/vim/vim/security/advisories/GHSA-3xx4-hcq6-r2vj, https://github.com/vim/vim/commit/ac63787734fda2e294e477af52b3bd601517fa78	O-FED-FEDO-191223/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.0.2108. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48233**		
Integer Overflow or Wraparound	16-Nov-2023	4.3	Vim is an open source command line text editor. When getting the count for a normal mode z command, it may overflow for large counts given. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `58f9befca1` which has been included in release version 9.0.2109. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48234**	https://github.com/vim/vim/security/advisories/GHSA-59gw-c949-6phq, https://github.com/vim/vim/commit/58f9befca1fa172068effad7f2ea5a9d6a7b0cca	O-FED-FEDO-191223/1251
Integer Overflow or Wraparound	16-Nov-2023	4.3	Vim is an open source command line text editor. When parsing relative ex addresses one may	https://github.com/vim/vim/security/advisories/GHSA-6g74-hr6q-pr8g, https://github.	O-FED-FEDO-191223/1252

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
			unintentionally cause an overflow. Ironically this happens in the existing overflow check, because the line number becomes negative and LONG_MAX - lnum will cause the overflow. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `060623e` which has been included in release version 9.0.2110. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48235**	com/vim/vim/commit/060623e4a3bc72b011e7cd92bedb3bfb64e06200	
Integer Overflow or Wraparound	16-Nov-2023	4.3	Vim is an open source command line text editor. When using the z= command, the user may overflow the count with values larger than MAX_INT. Impact is low, user interaction is required and a crash may not even	https://github.com/vim/vim/security/advisories/GHSA-pr4c-932v-8hx5, https://github.com/vim/vim/commit/73b2d3790cad5694fc0ed0db2926e4220c48d968	O-FED-FEDO-191223/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			happen in all situations. This vulnerability has been addressed in commit `73b2d379` which has been included in release version 9.0.2111. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-48236**		
Integer Overflow or Wraparound	16-Nov-2023	4.3	Vim is an open source command line text editor. In affected versions when shifting lines in operator pending mode and using a very large value, it may be possible to overflow the size of integer. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `6bf131888` which has been included in version 9.0.2112. Users are advised to upgrade. There are no known workarounds for this vulnerability.	https://github.com/vim/vim/security/advisories/GHSA-f2m2-v387-gv87, https://github.com/vim/vim/commit/6bf131888a3d1de62bbfa8a7ea03c0ddccfd496e	O-FED-FEDO-191223/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48237		
Vendor: Freebsd					
Product: freebsd					
Affected Version(s): 14.0					
Authorization Bypass Through User-Controlled Key	24-Nov-2023	7.5	OpenZFS through 2.1.13 and 2.2.x through 2.2.1, in certain scenarios involving applications that try to rely on efficient copying of file data, can replace file contents with zero-valued bytes and thus potentially disable security mechanisms. NOTE: this issue is not always security related, but can be security related in realistic situations. A possible example is cp, from a recent GNU Core Utilities (coreutils) version, when attempting to preserve a rule set for denying unauthorized access. (One might use cp when configuring access control, such as with the /etc/hosts.deny file specified in the IBM Support reference.) NOTE: this issue occurs less often in	https://github.com/openzfs/zfs/pull/15571, https://github.com/openzfs/zfs/issues/15526, https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=275308, https://news.ycombinator.com/item?id=38405731	O-FRE-FREE-191223/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 2.2.1, and in versions before 2.1.4, because of the default configuration in those versions. **CVE ID : CVE-2023-49298**		
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Incorrect Default Permissions	18-Nov-2023	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to change installation files due to incorrect file permission settings. IBM X-Force ID: 263332. **CVE ID : CVE-2023-40363**	https://exchange.xforce.ibmcloud.com/vulnerabilities/263332	O-IBM-AIX-191223/1256
Vendor: inea					
Product: me_rtu_firmware					
Affected Version(s): * Up to (excluding) 3.37					
Improper Authentication	20-Nov-2023	9.8	Versions of INEA ME RTU firmware 3.36b and prior do not require authentication to the "root" account on the host system of the device. This could allow an attacker to obtain admin-level access to the host system.	N/A	O-INE-ME_R-191223/1257

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-2023-29155		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Nov-2023	9.8	Versions of INEA ME RTU firmware 3.36b and prior are vulnerable to operating system (OS) command injection, which could allow remote code execution. **CVE ID : CVE-2023-35762**	N/A	O-INE-ME_R-191223/1258
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
NULL Pointer Dereference	16-Nov-2023	7.8	A null pointer dereference flaw was found in the Linux kernel API for the cryptographic algorithm scatterwalk functionality. This issue occurs when a user constructs a malicious packet with specific socket	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=cfaa80c91f6f99b9342b6557f0f0e1143e434066	O-LIN-LINU-191223/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration, which could allow a local user to crash the system or escalate their privileges on the system. **CVE ID : CVE-2023-6176**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Nov-2023	7.8	A buffer overflow vulnerability was found in the NVM Express (NVMe) driver in the Linux kernel. An unprivileged user could specify a small meta buffer and let the device perform larger Direct Memory Access (DMA) into the same buffer, overwriting unrelated kernel memory, causing random kernel crashes and memory corruption. **CVE ID : CVE-2023-6238**	N/A	O-LIN-LINU-191223/1260
N/A	18-Nov-2023	7.5	IBM CICS TX Advanced 10.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM	https://www.ibm.com/support/pages/node/7066431, https://exchange.xforce.ibmcloud.com/vulnerabilities/260770	O-LIN-LINU-191223/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X-Force ID: 260770. **CVE ID : CVE-2023-38361**		
Incorrect Default Permissions	18-Nov-2023	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to change installation files due to incorrect file permission settings. IBM X-Force ID: 263332. **CVE ID : CVE-2023-40363**	https://exchange.xforce.ibmcloud.com/vulnerabilities/263332	O-LIN-LINU-191223/1262
Affected Version(s): 6.2					
NULL Pointer Dereference	23-Nov-2023	7.8	A null pointer dereference flaw was found in the nft_inner.c functionality of netfilter in the Linux kernel. This issue could allow a local user to crash the system or escalate their privileges on the system. **CVE ID : CVE-2023-5972**	https://bugzilla.redhat.com/show_bug.cgi?id=2248189, https://github.com/torvalds/linux/commit/505ce0630ad5d31185695f8a29dde8d29f28faa7, https://github.com/torvalds/linux/commit/52177bbf19e6e9398375a148d2e13ed492b40b80	O-LIN-LINU-191223/1263
Affected Version(s): 6.2.0					
NULL Pointer Dereference	23-Nov-2023	7.8	A null pointer dereference flaw was found in the nft_inner.c functionality of netfilter in the	https://bugzilla.redhat.com/show_bug.cgi?id=2248189, https://github.com/torvalds/l	O-LIN-LINU-191223/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Linux kernel. This issue could allow a local user to crash the system or escalate their privileges on the system. **CVE ID : CVE-2023-5972**	inux/commit/505ce0630ad5d31185695f8a29dde8d29f28faa7, https://github.com/torvalds/linux/commit/52177bbf19e6e9398375a148d2e13ed492b40b80	
Affected Version(s): 6.6					
NULL Pointer Dereference	23-Nov-2023	7.8	A null pointer dereference flaw was found in the nft_inner.c functionality of netfilter in the Linux kernel. This issue could allow a local user to crash the system or escalate their privileges on the system. **CVE ID : CVE-2023-5972**	https://bugzilla.redhat.com/show_bug.cgi?id=2248189, https://github.com/torvalds/linux/commit/505ce0630ad5d31185695f8a29dde8d29f28faa7, https://github.com/torvalds/linux/commit/52177bbf19e6e9398375a148d2e13ed492b40b80	O-LIN-LINU-191223/1265
Affected Version(s): From (including) 6.2.1 Up to (including) 6.5.10					
NULL Pointer Dereference	23-Nov-2023	7.8	A null pointer dereference flaw was found in the nft_inner.c functionality of netfilter in the Linux kernel. This issue could allow a local user to crash the system or escalate their	https://bugzilla.redhat.com/show_bug.cgi?id=2248189, https://github.com/torvalds/linux/commit/505ce0630ad5d31185695f8a29dde8d29f28faa7,	O-LIN-LINU-191223/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on the system. **CVE ID : CVE-2023-5972**	https://github.com/torvalds/linux/commit/52177bbf19e6e9398375a148d2e13ed492b40b80	
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Improper Authentication	17-Nov-2023	9.8	Adobe FrameMaker versions 2022 and earlier are affected by an Improper Authentication vulnerability that could result in a Security feature bypass. An unauthenticated attacker can abuse this vulnerability to access the API and leak default admin's password. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-44324**	https://helpx.adobe.com/security/products/framemaker/apsb23-58.html	O-MIC-WIND-191223/1267
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-MIC-WIND-191223/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47066**		
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47067**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-MIC-WIND-191223/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47068**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-MIC-WIND-191223/1270
Out-of-bounds Read	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-MIC-WIND-191223/1271

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-2023-47069**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe InCopy versions 18.5 (and earlier) and 17.4.2 (and earlier) are affected by 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-2023-26368**	https://helpx.adobe.com/security/products/incopy/apsb23-60.html	O-MIC-WIND-191223/1272
Out-of-bounds Write	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds write vulnerability that	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-MIC-WIND-191223/1273

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
			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-2023-47070**		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44366**	N/A	O-MIC-WIND-191223/1274
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	O-MIC-WIND-191223/1275

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-2023-47041**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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-2023-47058**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-MIC-WIND-191223/1276
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds write vulnerability	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-MIC-WIND-191223/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47057**		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (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-2023-47056**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-MIC-WIND-191223/1278
Use After Free	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-MIC-WIND-191223/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47055**		
Out-of-bounds Write	17-Nov-2023	7.8	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (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-2023-47073**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-MIC-WIND-191223/1280
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (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	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-MIC-WIND-191223/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-44330**		
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47051**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-MIC-WIND-191223/1282
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-MIC-WIND-191223/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47050**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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-2023-47049**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-MIC-WIND-191223/1284
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are	https://helpx.adobe.com/security/products/	O-MIC-WIND-191223/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47048**	audition/apsb23-64.html	
Access of Uninitialized Pointer	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-47047**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-MIC-WIND-191223/1286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44336**	N/A	O-MIC-WIND-191223/1287
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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	N/A	O-MIC-WIND-191223/1288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44337**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44338**	N/A	O-MIC-WIND-191223/1289
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Audition version 24.0 (and earlier) and 23.6.1 (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/audition/apsb23-64.html	O-MIC-WIND-191223/1290

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-2023-47046**		
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (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-2023-47043**	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	O-MIC-WIND-191223/1291
Out-of-bounds Write	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by a Heap-based Buffer Overflow	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	O-MIC-WIND-191223/1292

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-2023-47042**		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44367**	N/A	O-MIC-WIND-191223/1293
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	O-MIC-WIND-191223/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47040**		
Uncontrolled Search Path Element	22-Nov-2023	7.8	A binary hijacking vulnerability exists within the VideoLAN VLC media player before 3.0.19 on Windows. The uninstaller attempts to execute code with elevated privileges out of a standard user writable location. Standard users may use this to gain arbitrary code execution as SYSTEM. **CVE ID : CVE-2023-46814**	https://www.videolan.org/security/sb-vlc3019.html	O-MIC-WIND-191223/1295
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected	N/A	O-MIC-WIND-191223/1296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-44359**		
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (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-2023-44372**	N/A	O-MIC-WIND-191223/1297
Use After Free	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by a Use After Free vulnerability that could result in	N/A	O-MIC-WIND-191223/1298

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-2023-44371**		
Access of Uninitialized Pointer	16-Nov-2023	7.8	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an Access of Uninitialized Pointer 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-2023-44365**	N/A	O-MIC-WIND-191223/1299
Out-of-bounds Read	16-Nov-2023	7.8	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-MIC-WIND-191223/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-47059**		
Improper Input Validation	17-Nov-2023	7.5	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Input Validation vulnerability that could lead to information disclosure by an unauthenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-22272**	https://helpx.adobe.com/security/products/robohelp-server/apsb23-53.html	O-MIC-WIND-191223/1301
Improper Restriction of XML External Entity Reference	17-Nov-2023	7.5	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that	https://helpx.adobe.com/security/products/robohelp-server/apsb23-53.html	O-MIC-WIND-191223/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to information disclosure by an unauthenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-22274**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Nov-2023	7.5	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead to information disclosure by an unauthenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-22275**	https://helpx.adobe.com/security/products/robohelp-server/apsb23-53.html	O-MIC-WIND-191223/1303
Improper Link Resolution Before File Access ('Link Following')	16-Nov-2023	7.3	Dell Encryption, Dell Endpoint Security Suite Enterprise, and Dell Security Management Server version prior to 11.8.1	https://www.dell.com/support/kbdoc/en-us/000217572/dsa-2023-271	O-MIC-WIND-191223/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain an Insecure Operation on Windows Junction Vulnerability during installation. A local malicious user could potentially exploit this vulnerability to create an arbitrary folder inside a restricted directory, leading to Privilege Escalation **CVE ID : CVE-2023-39246**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Nov-2023	7.2	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to Remote Code Execution by an admin authenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-22273**	https://helpx.adobe.com/security/products/robohelp-server/apsb23-53.html	O-MIC-WIND-191223/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	6.5	Path traversal vulnerability whose exploitation could allow an authenticated remote user to bypass SecurityManager's intended restrictions and list a parent directory via any filename, such as a multiple ..%2F value affecting the 'dodoc' parameter in the /MailAdmin_dll.htm file. **CVE ID : CVE-2023-4593**	N/A	O-MIC-WIND-191223/1306
Insertion of Sensitive Information into Externally-Accessible File or Directory	23-Nov-2023	6.5	An information exposure vulnerability has been found, the exploitation of which could allow a remote user to retrieve sensitive information stored on the server such as credential files, configuration files, application files, etc., simply by appending any of the following parameters to the end of the URL: %00 %0a, %20, %2a, %a0, %aa, %c0 and %ca.	N/A	O-MIC-WIND-191223/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4595		
Incorrect Default Permissions	18-Nov-2023	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to change installation files due to incorrect file permission settings. IBM X-Force ID: 263332. **CVE ID : CVE-2023-40363**	https://exchange.xforce.ibmcloud.com/vulnerabilities/263332	O-MIC-WIND-191223/1308
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Nov-2023	6.5	Adobe RoboHelp Server versions 11.4 and earlier are affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead to information disclosure by an low-privileged authenticated attacker. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-22268**	https://helpx.adobe.com/security/products/robohelp-server/apsb23-53.html	O-MIC-WIND-191223/1309
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and	N/A	O-MIC-WIND-191223/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44348**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44340**	N/A	O-MIC-WIND-191223/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Media Encoder version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47044**	https://helpx.adobe.com/security/products/media-encoder/apsb23-63.html	O-MIC-WIND-191223/1312
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-MIC-WIND-191223/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-44335**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44334**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-MIC-WIND-191223/1314
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-MIC-WIND-191223/1315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44333**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44332**	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-MIC-WIND-191223/1316
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Photoshop versions 24.7.1 (and earlier) and 25.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this	https://helpx.adobe.com/security/products/photoshop/apsb23-56.html	O-MIC-WIND-191223/1317

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
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44331**		
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44329**	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	O-MIC-WIND-191223/1318
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-MIC-WIND-191223/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47053**		
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47054**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-MIC-WIND-191223/1320
Use After Free	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by a Use After Free vulnerability that could lead to	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	O-MIC-WIND-191223/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44328**		
Access of Uninitialized Pointer	16-Nov-2023	5.5	Adobe Bridge versions 13.0.4 (and earlier) and 14.0.0 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44327**	https://helpx.adobe.com/security/products/bridge/apsb23-57.html	O-MIC-WIND-191223/1322
Out-of-bounds Read	17-Nov-2023	5.5	Adobe Dimension versions 3.4.9 (and earlier) is affected by an out-of-bounds read	https://helpx.adobe.com/security/products/	O-MIC-WIND-191223/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44326**	dimension/apsb23-62.html	
Out-of-bounds Read	17-Nov-2023	5.5	Adobe Animate versions 23.0.2 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44325**	https://helpx.adobe.com/security/products/animate/apsb23-61.html	O-MIC-WIND-191223/1324
Use After Free	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected	N/A	O-MIC-WIND-191223/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44361**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Audition version 24.0 (and earlier) and 23.6.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47052**	https://helpx.adobe.com/security/products/audition/apsb23-64.html	O-MIC-WIND-191223/1326
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and	N/A	O-MIC-WIND-191223/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44360**		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	O-MIC-WIND-191223/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-44358		
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44357**	N/A	O-MIC-WIND-191223/1329
Out-of-bounds Read	16-Nov-2023	5.5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	N/A	O-MIC-WIND-191223/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44356**		
Out-of-bounds Read	17-Nov-2023	5.5	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47071**	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-MIC-WIND-191223/1331
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Nov-2023	5.4	Stored XSS vulnerability. This vulnerability could allow an attacker to store a malicious JavaScript payload via GET and POST methods on multiple parameters in the MailAdmin_dll.htm file.	N/A	O-MIC-WIND-191223/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4594		
Out-of-bounds Read	16-Nov-2023	5	Adobe Acrobat Reader versions 23.006.20360 (and earlier) and 20.005.30524 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-44339**	N/A	O-MIC-WIND-191223/1333
Access of Uninitialized Pointer	17-Nov-2023	3.3	Adobe After Effects version 24.0.2 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/after_effects/apsb23-66.html	O-MIC-WIND-191223/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47072**		
Access of Uninitialized Pointer	16-Nov-2023	3.3	Adobe Premiere Pro version 24.0 (and earlier) and 23.6 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-47060**	https://helpx.adobe.com/security/products/premiere_pro/apsb23-65.html	O-MIC-WIND-191223/1335
Vendor: neutron					
Product: ipc2224-sr3-npf-36_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP	N/A	O-NEU-IPC2-191223/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**		
Product: ipc2624-sr3-npf-36_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-IPC2-191223/1337
Product: neu-ipb210-28_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NEU--191223/1338
Product: neu-ipb410-28_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NEU--191223/1339
Product: neu-ipbm211_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NEU--191223/1340
Product: neu-ipbm411_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1.	N/A	O-NEU-NEU--191223/1341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6118		
Product: neu-ipd220-28_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NEU--191223/1342
Product: neu-ipdm221_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NEU--191223/1343
Product: neu-ipdm421_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation	23-Nov-2023	7.5	Path Traversal: '/../filedir'	N/A	O-NEU-NEU--191223/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**		
Product: ntl-bc-01w_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NTL--191223/1345
Product: ntl-bc-03-snm_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1.	N/A	O-NEU-NTL--191223/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6118		
Product: ntl-bc-03-snp_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NTL--191223/1347
Product: ntl-bc01-m_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NTL--191223/1348
Product: ntl-ip05-3mp_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute	N/A	O-NEU-NTL--191223/1349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**		
Product: ntl-pt-06wod-3mp_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NTL--191223/1350
Product: ntl-pt-09-wos-3mp_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NTL--191223/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ntl-pt-10-4gwos-3mp_firmware					
Affected Version(s): * Up to (excluding) b1130.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Nov-2023	7.5	Path Traversal: '/../filedir' vulnerability in Neutron IP Camera allows Absolute Path Traversal.This issue affects IP Camera: before b1130.1.0.1. **CVE ID : CVE-2023-6118**	N/A	O-NEU-NTL--191223/1352
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 6.0					
Uncontrolled Resource Consumption	24-Nov-2023	6.5	An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow a remote attacker to cause a denial of service via a craft input with size smaller than 379 KB. **CVE ID : CVE-2023-6277**	https://bugzilla.redhat.com/show_bug.cgi?id=2251311, https://gitlab.com/libtiff/libtiff/-/issues/614, https://gitlab.com/libtiff/libtiff/-/merge_requests/545	O-RED-ENTE-191223/1353
Out-of-bounds Read	16-Nov-2023	4.3	An out-of-bounds read vulnerability was found in the NVMe-oF/TCP subsystem in the Linux kernel. This flaw allows a remote attacker to send a crafted TCP	N/A	O-RED-ENTE-191223/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet, triggering a heap-based buffer overflow that results in kmalloc data to be printed (and potentially leaked) to the kernel ring buffer (dmesg). **CVE ID : CVE-2023-6121**		
Affected Version(s): 7.0					
Uncontrolled Resource Consumption	24-Nov-2023	6.5	An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow a remote attacker to cause a denial of service via a craft input with size smaller than 379 KB. **CVE ID : CVE-2023-6277**	https://bugzilla.redhat.com/show_bug.cgi?id=2251311, https://gitlab.com/libtiff/libtiff/-/issues/614, https://gitlab.com/libtiff/libtiff/-/merge_requests/545	O-RED-ENTE-191223/1355
Out-of-bounds Read	16-Nov-2023	4.3	An out-of-bounds read vulnerability was found in the NVMe-oF/TCP subsystem in the Linux kernel. This flaw allows a remote attacker to send a crafted TCP packet, triggering a heap-based buffer overflow that results in kmalloc data to be printed (and potentially leaked) to the	N/A	O-RED-ENTE-191223/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel ring buffer (dmesg). **CVE ID : CVE-2023-6121**		
Affected Version(s): 8.0					
NULL Pointer Dereference	16-Nov-2023	7.8	A null pointer dereference flaw was found in the Linux kernel API for the cryptographic algorithm scatterwalk functionality. This issue occurs when a user constructs a malicious packet with specific socket configuration, which could allow a local user to crash the system or escalate their privileges on the system. **CVE ID : CVE-2023-6176**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=cfaa80c91f6f99b9342b6557f0f0e1143e434066	O-RED-ENTE-191223/1357
Uncontrolled Resource Consumption	24-Nov-2023	6.5	An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow a remote attacker to cause a denial of service via a craft input with size smaller than 379 KB. **CVE ID : CVE-2023-6277**	https://bugzilla.redhat.com/show_bug.cgi?id=2251311, https://gitlab.com/libtiff/libtiff/-/issues/614, https://gitlab.com/libtiff/libtiff/-/merge_requests/545	O-RED-ENTE-191223/1358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Nov-2023	4.3	An out-of-bounds read vulnerability was found in the NVMe-oF/TCP subsystem in the Linux kernel. This flaw allows a remote attacker to send a crafted TCP packet, triggering a heap-based buffer overflow that results in kmalloc data to be printed (and potentially leaked) to the kernel ring buffer (dmesg). **CVE ID : CVE-2023-6121**	N/A	O-RED-ENTE-191223/1359
Affected Version(s): 9.0					
NULL Pointer Dereference	16-Nov-2023	7.8	A null pointer dereference flaw was found in the Linux kernel API for the cryptographic algorithm scatterwalk functionality. This issue occurs when a user constructs a malicious packet with specific socket configuration, which could allow a local user to crash the system or escalate their privileges on the system.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=cfaa80c91f6f99b9342b6557f0f0e1143e434066	O-RED-ENTE-191223/1360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6176		
Uncontrolled Resource Consumption	24-Nov-2023	6.5	An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow a remote attacker to cause a denial of service via a craft input with size smaller than 379 KB. **CVE ID : CVE-2023-6277**	https://bugzilla.redhat.com/show_bug.cgi?id=2251311, https://gitlab.com/libtiff/libtiff/-/issues/614, https://gitlab.com/libtiff/libtiff/-/merge_requests/545	O-RED-ENTE-191223/1361
Out-of-bounds Read	16-Nov-2023	4.3	An out-of-bounds read vulnerability was found in the NVMe-oF/TCP subsystem in the Linux kernel. This flaw allows a remote attacker to send a crafted TCP packet, triggering a heap-based buffer overflow that results in kmalloc data to be printed (and potentially leaked) to the kernel ring buffer (dmesg). **CVE ID : CVE-2023-6121**	N/A	O-RED-ENTE-191223/1362
Vendor: redlioncontrols					
Product: st-ipm-6350_firmware					
Affected Version(s): 4.9.114					
N/A	21-Nov-2023	9.8		https://support.redlion.net/hc/en-	O-RED-ST-I-191223/1363

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
			When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-40151**	us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	O-RED-ST-I-191223/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-42770**		
Product: st-ipm-8460_firmware					
Affected Version(s): 6.0.202					
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge.	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	O-RED-ST-I-191223/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40151		
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-42770**	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	O-RED-ST-I-191223/1366
Product: vt-ipm2m-113-d_firmware					
Affected Version(s): 4.9.114					
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	O-RED-VT-I-191223/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-40151**		
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge.	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	O-RED-VT-I-191223/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42770		
Product: vt-ipm2m-213-d_firmware					
Affected Version(s): 4.9.114					
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-40151**	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	O-RED-VT-I-191223/1369
Missing Authentication for	21-Nov-2023	9.8		https://https://support.redlion.net/hc/en-	O-RED-VT-I-191223/1370

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
Critical Function			Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-42770**	us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	
Product: vt-mipm-135-d_firmware					
Affected Version(s): 4.9.114					
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	O-RED-VT-M-191223/1371

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
			UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-40151**		
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-42770**	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	O-RED-VT-M-191223/1372
Product: vt-mipm-245-d_firmware					
Affected Version(s): 4.9.114					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Nov-2023	9.8	When user authentication is not enabled the shell can execute commands with the highest privileges. Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication challenge over UDP/IP. When the same message comes over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-40151**	https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-Remote-Code-Execution	O-RED-VT-M-191223/1373
Missing Authentication for Critical Function	21-Nov-2023	9.8	Red Lion SixTRAK and VersaTRAK Series RTUs with authenticated users enabled (UDR-A) any Sixnet UDR message will meet an authentication	https://https://support.redlion.net/hc/en-us/articles/19339209248269-RLCSIM-2023-05-Authentication-Bypass-and-	O-RED-VT-M-191223/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			challenge over UDP/IP. When the same message is received over TCP/IP the RTU will simply accept the message with no authentication challenge. **CVE ID : CVE-2023-42770**	Remote-Code-Execution	
Vendor: Tenda					
Product: ac10_firmware					
Affected Version(s): 16.03.10.13					
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the list parameter in the function sub_49E098. **CVE ID : CVE-2023-45479**	N/A	O-TEN-AC10-191223/1375
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the src parameter in the function sub_47D878. **CVE ID : CVE-2023-45480**	N/A	O-TEN-AC10-191223/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the firewallEn parameter in the function SetFirewallCfg. **CVE ID : CVE-2023-45481**	N/A	O-TEN-AC10-191223/1377
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the urls parameter in the function get_parentControl_list_Info. **CVE ID : CVE-2023-45482**	N/A	O-TEN-AC10-191223/1378
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the time parameter in the function compare_parentcontrol_time. **CVE ID : CVE-2023-45483**	N/A	O-TEN-AC10-191223/1379
Out-of-bounds Write	29-Nov-2023	9.8	Tenda AC10 version US_AC10V4.0si_V16	N/A	O-TEN-AC10-191223/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			.03.10.13_cn was discovered to contain a stack overflow via the shareSpeed parameter in the function fromSetWifiGuestBasic. **CVE ID : CVE-2023-45484**		
Product: ac18_firmware					
Affected Version(s): 15.03.05.19\\(6318\\)					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda Ac19 v.1.0, AC18, AC9 v.1.0, AC6 v.2.0 and v.1.0 allows a remote attacker to execute arbitrary code via the formSetCfm function in bin/httpd. **CVE ID : CVE-2023-38823**	N/A	O-TEN-AC18-191223/1381
Product: ac19_firmware					
Affected Version(s): 15.03.05.19\\(6318\\)					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda Ac19 v.1.0, AC18, AC9 v.1.0, AC6 v.2.0 and v.1.0 allows a remote attacker to execute arbitrary code via the formSetCfm function in bin/httpd. **CVE ID : CVE-2023-38823**	N/A	O-TEN-AC19-191223/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ac6_firmware					
Affected Version(s): 15.03.05.19\\(6318\\)					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda Ac19 v.1.0, AC18, AC9 v.1.0, AC6 v.2.0 and v.1.0 allows a remote attacker to execute arbitrary code via the formSetCfm function in bin/httpd. **CVE ID : CVE-2023-38823**	N/A	O-TEN-AC6_-191223/1383
Product: ac9_firmware					
Affected Version(s): 15.03.05.19\\(6318\\)					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda Ac19 v.1.0, AC18, AC9 v.1.0, AC6 v.2.0 and v.1.0 allows a remote attacker to execute arbitrary code via the formSetCfm function in bin/httpd. **CVE ID : CVE-2023-38823**	N/A	O-TEN-AC9_-191223/1384
Product: ax1803_firmware					
Affected Version(s): 1.0.0.1					
Out-of-bounds Write	27-Nov-2023	9.8	Buffer Overflow vulnerability in Tenda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the wpapsk_crypto parameter in the	N/A	O-TEN-AX18-191223/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function fromSetWirelessRepeat. **CVE ID : CVE-2023-49043**		
Out-of-bounds Write	27-Nov-2023	9.8	Stack Overflow vulnerability in Tenda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the ssid parameter in the function form_fast_setting_wifi_set. **CVE ID : CVE-2023-49044**	N/A	O-TEN-AX18-191223/1386
Out-of-bounds Write	27-Nov-2023	9.8	Stack Overflow vulnerability in Tenda AX1803 v.1.0.0.1 allows a remote attacker to execute arbitrary code via the devName parameter in the function formAddMacfilterRule. **CVE ID : CVE-2023-49046**	N/A	O-TEN-AX18-191223/1387
Out-of-bounds Write	20-Nov-2023	7.5	Tenda AX1803 v1.0.0.1 was discovered to contain a heap overflow via the deviceId parameter in the function saveParentControlInfo . This vulnerability allows	N/A	O-TEN-AX18-191223/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to cause a Denial of Service (DoS) attack **CVE ID : CVE-2023-48109**		
Out-of-bounds Write	20-Nov-2023	7.5	Tenda AX1803 v1.0.0.1 was discovered to contain a heap overflow via the urls parameter in the function saveParentControlInfo . This vulnerability allows attackers to cause a Denial of Service (DoS) attack **CVE ID : CVE-2023-48110**	N/A	O-TEN-AX18-191223/1389
Out-of-bounds Write	20-Nov-2023	7.5	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow via the time parameter in the function saveParentControlInfo . This vulnerability allows attackers to cause a Denial of Service (DoS) attack **CVE ID : CVE-2023-48111**	N/A	O-TEN-AX18-191223/1390
Vendor: totolink					
Product: a3700r_firmware					
Affected Version(s): 9.1.2u.6134_b20201202					
Improper Control of Generation	20-Nov-2023	7.8	An issue in TOTOlink A3700R v.9.1.2u.6134_B202	N/A	O-TOT-A370-191223/1391

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
of Code ('Code Injection')			01202 allows a local attacker to execute arbitrary code via the setTracerouteCfg function. **CVE ID : CVE-2023-48192**		
Vendor: tribe29					
Product: checkmk_appliance_firmware					
Affected Version(s): * Up to (excluding) 1.6.8					
Insertion of Sensitive Information into Log File	27-Nov-2023	5.5	Sensitive data exposure in Webconf in Tribe29 Checkmk Appliance before 1.6.8 allows local attacker to retrieve passwords via reading log files. **CVE ID : CVE-2023-6287**	https://checkmk.com/werk/9554	O-TRI-CHEC-191223/1392
Vendor: unitree					
Product: a1_firmware					
Affected Version(s): -					
Missing Authentication for Critical Function	22-Nov-2023	7.5	Lack of authentication vulnerability. An unauthenticated local user is able to see through the cameras using the web server due to the lack of any form of authentication. **CVE ID : CVE-2023-3104**	https://www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-unitree-robotics-a1	O-UNI-A1_F-191223/1393
N/A	22-Nov-2023	5.9	Authentication bypass vulnerability, the exploitation of	https://www.incibe.es/en/incibe-cert/notices/av	O-UNI-A1_F-191223/1394

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
			which could allow a local attacker to perform a Man-in-the-Middle (MITM) attack on the robot's camera video stream. In addition, if a MITM attack is carried out, it is possible to consume the robot's resources, which could lead to a denial-of-service (DOS) condition. **CVE ID : CVE-2023-3103**	iso/multiple-vulnerabilities-unitree-robotics-a1	
Vendor: Wago					
Product: 0852-0602_firmware					
Affected Version(s): * Up to (excluding) 1.0.6.s0					
N/A	21-Nov-2023	0	A vulnerability in the web-based management allows an unauthenticated remote attacker to inject arbitrary system commands and gain full system control. Those commands are executed with root privileges. The vulnerability is located in the user request handling of the web-based management. **CVE ID : CVE-2023-4149**	N/A	O-WAG-0852-191223/1395
Product: 0852-0603_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.0.6.s0					
N/A	21-Nov-2023	0	A vulnerability in the web-based management allows an unauthenticated remote attacker to inject arbitrary system commands and gain full system control. Those commands are executed with root privileges. The vulnerability is located in the user request handling of the web-based management. **CVE ID : CVE-2023-4149**	N/A	O-WAG-0852-191223/1396
Product: 0852-1605_firmware					
Affected Version(s): * Up to (excluding) 1.2.5.s0					
N/A	21-Nov-2023	0	A vulnerability in the web-based management allows an unauthenticated remote attacker to inject arbitrary system commands and gain full system control. Those commands are executed with root privileges. The vulnerability is located in the user request handling of the web-based management.	N/A	O-WAG-0852-191223/1397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-4149		
Product: compact_controller_100_firmware					
Affected Version(s): * Up to (including) 25					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	O-WAG-COMP-191223/1398
Product: edge_controller_firmware					
Affected Version(s): * Up to (including) 25					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	O-WAG-EDGE-191223/1399
Product: pfc100_firmware					
Affected Version(s): * Up to (excluding) 22					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability	N/A	O-WAG-PFC1-191223/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**		
Affected Version(s): 22					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	O-WAG-PFC1-191223/1401
Product: pfc200_firmware					
Affected Version(s): * Up to (excluding) 22					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	O-WAG-PFC2-191223/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 22					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	O-WAG-PFC2-191223/1403
Affected Version(s): 23					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	O-WAG-PFC2-191223/1404
Affected Version(s): 24					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to	N/A	O-WAG-PFC2-191223/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate non-root privileges. **CVE ID : CVE-2023-3379**		
Product: touch_panel_600_advanced_firmware					
Affected Version(s): * Up to (including) 25					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	O-WAG-TOUC-191223/1406
Product: touch_panel_600_marine_firmware					
Affected Version(s): * Up to (including) 25					
N/A	20-Nov-2023	0	Wago web-based management of multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**	N/A	O-WAG-TOUC-191223/1407
Product: touch_panel_600_standard_firmware					
Affected Version(s): * Up to (including) 25					
N/A	20-Nov-2023	0	Wago web-based management of	N/A	O-WAG-TOUC-191223/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple products has a vulnerability which allows an local authenticated attacker to change the passwords of other non-admin users and thus to escalate non-root privileges. **CVE ID : CVE-2023-3379**		
Vendor: zephyrproject					
Product: zephyr					
Affected Version(s): * Up to (including) 3.4.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Nov-2023	8.8	An malicious BLE device can cause buffer overflow by sending malformed advertising packet BLE device using Zephyr OS, leading to DoS or potential RCE on the victim BLE device. **CVE ID : CVE-2023-4424**	N/A	O-ZEP-ZEPH-191223/1409