National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 - 28 Feb 2023 Vol. 10 No. 04

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: add_user_project					
Product: add_user					
Affected Version(s): * Up to (including) 2.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	6.1	The Custom Add User WordPress plugin through 2.0.2 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 against high privilege users such as admin **CVE ID : CVE-2023-0043**	N/A	A-ADD-ADD_-160323/1
Vendor: Adobe					
Product: after_effects					
Affected Version(s): From (including) 22.0.0 Up to (excluding) 22.6.4					
Out-of-bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	A-ADO-AFTE-160323/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22237		
Out-of-bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (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-2023-22238**	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	A-ADO-AFTE-160323/3
Improper Input Validation	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an Improper Input Validation 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-2023-22239**	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	A-ADO-AFTE-160323/4
Out-of-bounds Read	17-Feb-2023	5.5	After Affects versions 23.1 (and earlier), 22.6.3 (and	https://helpx.adobe.com/security/produc	A-ADO-AFTE-160323/5

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-2023-22233**	ts/after_effects/apsb23-02.html	
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.2.0					
Out-of-bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (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-2023-22237**	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	A-ADO-AFTE-160323/6
Out-of-bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds	https://helpx.adobe.com/security/products/after_effect	A-ADO-AFTE-160323/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-22238**	s/apsb23-02.html	
Improper Input Validation	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an Improper Input Validation 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-2023-22239**	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	A-ADO-AFTE-160323/8
Out-of-bounds Read	17-Feb-2023	5.5	After Affects versions 23.1 (and earlier), 22.6.3 (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/after_effects/apsb23-02.html	A-ADO-AFTE-160323/9

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-2023-22233**		
Product: animate					
Affected Version(s): 23.0.0					
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (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-2023-22236**	https://helpx.adobe.com/security/products/animate/apsb23-15.html	A-ADO-ANIM-160323/10
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/animate/apsb23-15.html	A-ADO-ANIM-160323/11

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-2023-22243**		
Use After Free	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (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-2023-22246**	https://helpx.adobe.com/security/products/animate/apsb23-15.html	A-ADO-ANIM-160323/12
Affected Version(s): From (including) 22.0.0 Up to (including) 22.0.8					
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/animate/apsb23-15.html	A-ADO-ANIM-160323/13

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-2023-22236**		
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Stack-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-2023-22243**	https://helpx.adobe.com/security/products/animate/apsb23-15.html	A-ADO-ANIM-160323/14
Use After Free	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (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	https://helpx.adobe.com/security/products/animate/apsb23-15.html	A-ADO-ANIM-160323/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-22246**		
Product: bridge					
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.0.4					
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by a Stack-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-2023-22226**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/16
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-22227**		
Improper Input Validation	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an Improper Input Validation 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-2023-22228**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/18
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22229		
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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-2023-22230**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/20
Out-of-bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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/bridge/apsb23-09.html	A-ADO-BRID-160323/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21583		
Out-of-bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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-2023-22231**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/22
Affected Version(s): From (including) 13.0.0 Up to (excluding) 13.0.2					
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by a Stack-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/bridge/apsb23-09.html	A-ADO-BRID-160323/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-22226**		
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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-2023-22227**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/24
Improper Input Validation	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22228		
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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-2023-22229**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/26
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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-2023-22230**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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-2023-21583**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	A-ADO-BRID-160323/28
Out-of-bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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/bridge/apsb23-09.html	A-ADO-BRID-160323/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22231		
Product: connect					
Affected Version(s): From (including) 11.0 Up to (including) 11.4.5					
N/A	17-Feb-2023	5.3	Adobe Connect versions 11.4.5 (and earlier), 12.1.5 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to impact the integrity of a minor feature. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-22232**	https://helpx.adobe.com/security/products/connect/apsb23-05.html	A-ADO-CONN-160323/30
Affected Version(s): From (including) 12.0 Up to (including) 12.1.5					
N/A	17-Feb-2023	5.3	Adobe Connect versions 11.4.5 (and earlier), 12.1.5 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to impact the integrity of a minor feature. Exploitation of this issue does not	https://helpx.adobe.com/security/products/connect/apsb23-05.html	A-ADO-CONN-160323/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			require user interaction. **CVE ID : CVE-2023-22232**		
Product: framemaker					
Affected Version(s): * Up to (including) 2020.0.4					
Out-of-bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (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-2023-21619**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	A-ADO-FRAM-160323/32
Improper Input Validation	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	A-ADO-FRAM-160323/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21621		
Out-of-bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (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-2023-21622**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	A-ADO-FRAM-160323/34
Use After Free	17-Feb-2023	5.5	FrameMaker 2020 Update 4 (and earlier), 2022 (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-2023-21584**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	A-ADO-FRAM-160323/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	17-Feb-2023	5.5	FrameMaker 2020 Update 4 (and earlier), 2022 (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-2023-21620**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	A-ADO-FRAM-160323/36
Affected Version(s): 2022					
Out-of-bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (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-2023-21619**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	A-ADO-FRAM-160323/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an Improper Input Validation 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-2023-21621**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	A-ADO-FRAM-160323/38
Out-of-bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (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-2023-21622**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	A-ADO-FRAM-160323/39
Use After Free	17-Feb-2023	5.5	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by a Use After Free vulnerability that	https://helpx.adobe.com/security/products/framemake	A-ADO-FRAM-160323/40

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-2023-21584**	r/apsb23-06.html	
Out-of-bounds Read	17-Feb-2023	5.5	FrameMaker 2020 Update 4 (and earlier), 2022 (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-2023-21620**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	A-ADO-FRAM-160323/41
Product: indesign					
Affected Version(s): 18.0					
NULL Pointer Dereference	17-Feb-2023	5.5	Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are	https://helpx.adobe.com/security/products/indesign/a	A-ADO-INDE-160323/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2023-21593**	psb23-12.html	
Affected Version(s): 18.1					
NULL Pointer Dereference	17-Feb-2023	5.5	Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2023-21593**	https://helpx.adobe.com/security/products/indesign/apsb23-12.html	A-ADO-INDE-160323/43
Affected Version(s): From (including) 17.0 Up to (including) 17.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	17-Feb-2023	5.5	Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2023-21593**	https://helpx.adobe.com/security/products/indesign/apsb23-12.html	A-ADO-INDE-160323/44
Product: photoshop					
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.5.4					
Improper Input Validation	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	A-ADO-PHOT-160323/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21574		
Out-of-bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (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-2023-21575**	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	A-ADO-PHOT-160323/46
Out-of-bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (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-2023-21576**	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	A-ADO-PHOT-160323/47
Out-of-bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of-	https://helpx.adobe.com/security/products/photoshop	A-ADO-PHOT-160323/48

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-2023-21577**	/apsb23-11.html	
Out-of-bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (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-2023-21578**	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	A-ADO-PHOT-160323/49
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.1.1					
Improper Input Validation	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are	https://helpx.adobe.com/security/produc	A-ADO-PHOT-160323/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Improper Input Validation 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-2023-21574**	ts/photoshop/apsb23-11.html	
Out-of-bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (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-2023-21575**	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	A-ADO-PHOT-160323/51
Out-of-bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (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/photoshop/apsb23-11.html	A-ADO-PHOT-160323/52

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-2023-21576**		
Out-of-bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (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-2023-21577**	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	A-ADO-PHOT-160323/53
Out-of-bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (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	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	A-ADO-PHOT-160323/54

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-2023-21578**		
Product: premiere_rush					
Affected Version(s): * Up to (including) 2.6					
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Premiere Rush version 2.6 (and earlier) is affected by a Stack-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-2023-22234**	https://helpx.adobe.com/security/products/premiere_rush/apsb23-14.html	A-ADO-PREM-160323/55
Use After Free	17-Feb-2023	7.8	Adobe Premiere Rush version 2.6 (and earlier) is 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	https://helpx.adobe.com/security/products/premiere_rush/apsb23-14.html	A-ADO-PREM-160323/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-22244**		
Vendor: afl\+\+_project					
Product: afl\+\+					
Affected Version(s): 4.05c					
N/A	21-Feb-2023	9.8	In AFL++ 4.05c, the CmpLog component uses the current working directory to resolve and execute unprefixed fuzzing targets, allowing code execution. **CVE ID : CVE-2023-26266**	https://github.com/AFLplusplus/AFLplusplus/pull/1643	A-AFL-AFL\-160323/57
Vendor: aioseo					
Product: all_in_one_seo					
Affected Version(s): * Up to (including) 4.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2023	5.4	The All in One SEO Pack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in versions up to, and including, 4.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Contributor+ role to inject arbitrary web scripts in pages that will execute whenever a user	N/A	A-AIO-ALL_-160323/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accesses an injected page. **CVE ID : CVE-2023-0586**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2023	4.8	The All in One SEO Pack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters in versions up to, and including, 4.2.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Administrator role or above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-0585**	N/A	A-AIO-ALL_-160323/59
Vendor: alphaware_simple_e-commerce_system_project					
Product: alphaware_simple_e-commerce_system					
Affected Version(s): 1.0					
Improper Access Control	24-Feb-2023	5.3	A vulnerability classified as critical has been found in SourceCodester Alphaware Simple E-Commerce System 1.0. This affects an unknown part of the file /alphaware/summary.php of the	N/A	A-ALP-ALPH-160323/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component Payment Handler. The manipulation of the argument amount leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221733 was assigned to this vulnerability. **CVE ID : CVE-2023-0998**		
Vendor: answer					
Product: answer					
Affected Version(s): * Up to (excluding) 1.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.5. **CVE ID : CVE-2023-0934**	https://huntr.dev/bounties/cd213098-5bab-487f-82c7-13698ad43b51, https://github.com/answerdev/answer/commit/edc06942d51fa8e56a134c5c7e5c8826d9260da0	A-ANS-ANSW-160323/61
Vendor: Apache					
Product: airflow_hive_provider					
Affected Version(s): * Up to (excluding) 5.1.3					
Improper Input Validation	24-Feb-2023	9.8	Improper Input Validation vulnerability in the Apache Airflow Hive	https://github.com/apache/airflow/pull/29502,	A-APA-AIRF-160323/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Provider. This issue affects Apache Airflow Hive Provider versions before 5.1.3. **CVE ID : CVE-2023-25696**	https://lists.apache.org/thread/99g0qm56wmgdxmbtdsvhj4rdnxhpzpml	
Product: airflow_sqoop_provider					
Affected Version(s): * Up to (excluding) 3.1.1					
Improper Input Validation	24-Feb-2023	9.8	Improper Input Validation vulnerability in the Apache Airflow Sqoop Provider. This issue affects Apache Airflow Sqoop Provider versions before 3.1.1. **CVE ID : CVE-2023-25693**	https://lists.apache.org/thread/79qn8g5xbq036f8crb115obvr22l52q4, https://github.com/apache/airflow/pull/29500	A-APA-AIRF-160323/63
Product: apache-airflow-providers-amazon					
Affected Version(s): * Up to (excluding) 7.2.1					
Generation of Error Message Containing Sensitive Information	24-Feb-2023	7.5	Generation of Error Message Containing Sensitive Information vulnerability in the Apache Airflow AWS Provider. This issue affects Apache Airflow AWS Provider versions before 7.2.1. **CVE ID : CVE-2023-25956**	https://lists.apache.org/thread/07pl9y4gdpw2c6rzqm77dvkm2z2kb5gv, https://github.com/apache/airflow/pull/29587	A-APA-APAC-160323/64
Product: apache-airflow-providers-google					
Affected Version(s): * Up to (excluding) 8.10.0					
Improper Input Validation	24-Feb-2023	9.8	Improper Input Validation vulnerability in the	https://lists.apache.org/thread/zdr8ovftt	A-APA-APAC-160323/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Apache Airflow Google Provider. This issue affects Apache Airflow Google Provider versions before 8.10.0. **CVE ID : CVE-2023-25691**	bh7kj0lydgcw88tbt2nmkcy, https://github.com/apache/airflow/pull/29497	
Improper Input Validation	24-Feb-2023	7.5	Improper Input Validation vulnerability in the Apache Airflow Google Provider. This issue affects Apache Airflow Google Provider versions before 8.10.0. **CVE ID : CVE-2023-25692**	https://lists.apache.org/thread/ks4l78l5rwdpmvfn7y7yhs179nyxtlsh, https://github.com/apache/airflow/pull/29499	A-APA-APAC-160323/66
Product: commons_fileupload					
Affected Version(s): 1.0					
Allocation of Resources Without Limits or Throttling	20-Feb-2023	7.5	Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads. Note that, like all of the file upload limits, the new configuration option (FileUploadBase#setFileCountMax) is not enabled by default	https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrrdoy	A-APA-COMM-160323/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and must be explicitly configured. **CVE ID : CVE-2023-24998**		
Affected Version(s): From (including) 1.0 Up to (excluding) 1.5					
Allocation of Resources Without Limits or Throttling	20-Feb-2023	7.5	Apache Commons FileUpload before 1.5 does not limit the number of request parts to be processed resulting in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads. Note that, like all of the file upload limits, the new configuration option (FileUploadBase#setFileCountMax) is not enabled by default and must be explicitly configured. **CVE ID : CVE-2023-24998**	https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrrdoy	A-APA-COMM-160323/68
Product: kerby					
Affected Version(s): * Up to (excluding) 2.0.3					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	20-Feb-2023	9.8	An LDAP Injection vulnerability exists in the LdapIdentityBackend of Apache Kerby before 2.0.3. **CVE ID : CVE-2023-25613**	N/A	A-APA-KERB-160323/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')					
Product: sling_i18n					
Affected Version(s): * Up to (excluding) 2.6.2					
N/A	23-Feb-2023	6.5	Privilege Escalation vulnerability in Apache Software Foundation Apache Sling. Any content author is able to create i18n dictionaries in the repository in a location the author has write access to. As these translations are used across the whole product, it allows an author to change any text or dialog in the product. For example an attacker might fool someone by changing the text on a delete button to "Info". This issue affects the i18n module of Apache Sling up to version 2.5.18. Version 2.6.2 and higher limit by default i18m dictionaries to certain paths in the repository (/libs and /apps). Users of the module are advised to update to version 2.6.2 or higher, check the configuration for resource loading and then adjust the	N/A	A-APA-SLIN-160323/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access permissions for the configured path accordingly. **CVE ID : CVE-2023-25621**		
Vendor: api-platform					
Product: core					
Affected Version(s): From (including) 2.6.0 Up to (excluding) 2.7.10					
Incorrect Authorization	28-Feb-2023	6.5	API Platform Core is the server component of API Platform: hypermedia and GraphQL APIs. Resource properties secured with the `security` option of the `ApiPlatform\Metadata\ApiProperty` attribute can be disclosed to unauthorized users. The problem affects most serialization formats, including raw JSON, which is enabled by default when installing API Platform. Custom serialization formats may also be impacted. Only collection endpoints are affected by the issue, item endpoints are not. The JSON-LD format is not affected by the issue. The result of the security rule is only executed for the first item of	https://github.com/api-platform/core/commit/5723d68369722feefeb11e42528d9580db5dd0fb, https://github.com/api-platform/core/security/advisories/GHSA-vr2x-7687-h6qv	A-API-CORE-160323/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the collection. The result of the rule is then cached and reused for the next items. This bug can leak data to unauthorized users when the rule depends on the value of a property of the item. This bug can also hide properties that should be displayed to authorized users. This issue impacts the 2.7, 3.0 and 3.1 branches. Please upgrade to versions 2.7.10, 3.0.12 or 3.1.3. As a workaround, replace the `cache_key` of the context array of the Serializer inside a custom normalizer that works on objects if the security option of the `ApiPlatform\Metadata\ApiProperty` attribute is used. **CVE ID : CVE-2023-25575**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.12					
Incorrect Authorization	28-Feb-2023	6.5	API Platform Core is the server component of API Platform: hypermedia and GraphQL APIs. Resource properties secured with the	https://github.com/api-platform/core/commit/5723d68369722feefeb11e42528d9580db5dd0fb,	A-API-CORE-160323/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`security` option of the `ApiPlatform\Metadata\ApiProperty` attribute can be disclosed to unauthorized users. The problem affects most serialization formats, including raw JSON, which is enabled by default when installing API Platform. Custom serialization formats may also be impacted. Only collection endpoints are affected by the issue, item endpoints are not. The JSON-LD format is not affected by the issue. The result of the security rule is only executed for the first item of the collection. The result of the rule is then cached and reused for the next items. This bug can leak data to unauthorized users when the rule depends on the value of a property of the item. This bug can also hide properties that should be displayed to authorized users. This issue impacts the 2.7, 3.0 and 3.1 branches. Please	https://github.com/api-platform/core/security/advisories/GHSA-vr2x-7687-h6qv	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade to versions 2.7.10, 3.0.12 or 3.1.3. As a workaround, replace the `cache_key` of the context array of the Serializer inside a custom normalizer that works on objects if the security option of the `ApiPlatform\Metadata\ApiProperty` attribute is used. **CVE ID : CVE-2023-25575**		
Affected Version(s): From (including) 3.1.0 Up to (excluding) 3.1.3					
Incorrect Authorization	28-Feb-2023	6.5	API Platform Core is the server component of API Platform: hypermedia and GraphQL APIs. Resource properties secured with the `security` option of the `ApiPlatform\Metadata\ApiProperty` attribute can be disclosed to unauthorized users. The problem affects most serialization formats, including raw JSON, which is enabled by default when installing API Platform. Custom serialization formats may also be impacted. Only collection endpoints	https://github.com/api-platform/core/commit/5723d68369722feefeb11e42528d9580db5dd0fb, https://github.com/api-platform/core/security/advisories/GHSA-vr2x-7687-h6qv	A-API-CORE-160323/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected by the issue, item endpoints are not. The JSON-LD format is not affected by the issue. The result of the security rule is only executed for the first item of the collection. The result of the rule is then cached and reused for the next items. This bug can leak data to unauthorized users when the rule depends on the value of a property of the item. This bug can also hide properties that should be displayed to authorized users. This issue impacts the 2.7, 3.0 and 3.1 branches. Please upgrade to versions 2.7.10, 3.0.12 or 3.1.3. As a workaround, replace the `cache_key` of the context array of the Serializer inside a custom normalizer that works on objects if the security option of the `ApiPlatform\Metadata\ApiProperty` attribute is used. **CVE ID : CVE-2023-25575**		
Vendor: apolloconfig					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: apollo					
Affected Version(s): * Up to (excluding) 2.1.0					
Missing Authentication for Critical Function	20-Feb-2023	7.5	Apollo is a configuration management system. Prior to version 2.1.0, there are potential security issues if users expose apollo-configservice to the internet, which is not recommended. This is because there is no authentication feature enabled for the built-in eureka service. Malicious hackers may access eureka directly to mock apollo-configservice and apollo-adminservice. Login authentication for eureka was added in version 2.1.0. As a workaround, avoid exposing apollo-configservice to the internet. **CVE ID : CVE-2023-25570**	https://github.com/apolloconfig/apollo/pull/4663, https://github.com/apolloconfig/apollo/commit/7df79bf8df6960433ed4ff782a54e3dfc74632bd	A-APO-APOL-160323/74
Cross-Site Request Forgery (CSRF)	20-Feb-2023	5.7	Apollo is a configuration management system. Prior to version 2.1.0, a low-privileged user can create a special web page. If an authenticated portal admin visits this	https://github.com/apolloconfig/apollo/pull/4664, https://github.com/apolloconfig/apollo/commit/00d968a7229f809b0d8ed0532e8c	A-APO-APOL-160323/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page, the page can silently send a request to assign new roles for that user without any confirmation from the Portal admin. Cookie SameSite strategy was set to Lax in version 2.1.0. As a workaround, avoid visiting unknown source pages. **CVE ID : CVE-2023-25569**	01a6c2b7c750	
Vendor: Apple					
Product: safari					
Affected Version(s): * Up to (excluding) 16.3					
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23496**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599, https://support.apple.com/	A-APP-SAFA-160323/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213600	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23517**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	A-APP-SAFA-160323/77
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/	A-APP-SAFA-160323/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23518**	en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
Access of Resource Using Incompatible Type ('Type Confusion')	27-Feb-2023	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, Safari 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2023-23529**	https://support.apple.com/en-us/HT213638, https://support.apple.com/en-us/HT213635, https://support.apple.com/en-us/HT213633	A-APP-SAFA-160323/79
Vendor: apusthemes					
Product: wp_private_messaging					
Affected Version(s): * Up to (excluding) 1.0.6					
Authorization Bypass Through	21-Feb-2023	4.3	The WP Private Message WordPress plugin (bundled with	N/A	A-APU-WP_P-160323/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
User-Controlled Key			the Superio theme as a required plugin) before 1.0.6 does not ensure that private messages to be accessed belong to the user making the requests. This allowing any authenticated users to access private messages belonging to other users by tampering the ID. **CVE ID : CVE-2023-0453**		
Vendor: artisanworkshop					
Product: japanized_for_woocommerce					
Affected Version(s): * Up to (including) 2.5.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	The Japanized For WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in versions up to, and including, 2.5.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2868545%40woocommerce-for-japan%2Ftrunk&old=2863064%40woocommerce-for-japan%2Ftrunk&sfp_email=&sfph_mail=	A-ART-JAPA-160323/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0942		
Vendor: art_gallery_management_system_project					
Product: art_gallery_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	9.8	Art Gallery Management System Project in PHP 1.0 was discovered to contain a SQL injection vulnerability via the username parameter in the Admin Login. **CVE ID : CVE-2023-23155**	N/A	A-ART-ART_-160323/82
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	9.8	Art Gallery Management System Project in PHP 1.0 was discovered to contain a SQL injection vulnerability via the pid parameter in the single-product page. **CVE ID : CVE-2023-23156**	N/A	A-ART-ART_-160323/83
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	A stored cross-site scripting (XSS) vulnerability in Art Gallery Management System Project v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the fullname parameter on the enquiry page. **CVE ID : CVE-2023-23157**	N/A	A-ART-ART_-160323/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	A stored cross-site scripting (XSS) vulnerability in Art Gallery Management System Project v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the message parameter on the enquiry page. **CVE ID : CVE-2023-23158**	N/A	A-ART-ART_-160323/85
Vendor: automatorwp					
Product: automatorwp					
Affected Version(s): * Up to (excluding) 2.5.1					
Cross-Site Request Forgery (CSRF)	28-Feb-2023	4.3	Cross-Site Request Forgery (CSRF) vulnerability in AutomatorWP plugin <= 2.5.0 leads to object delete. **CVE ID : CVE-2023-23992**	N/A	A-AUT-AUTO-160323/86
Vendor: auto_dealer_management_system_project					
Product: auto_dealer_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2023	8.8	A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. This affects an unknown part of the file /adms/admin/?page=vehicles/view_transaction. The manipulation of the argument id leads to	N/A	A-AUT-AUTO-160323/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221481 was assigned to this vulnerability. **CVE ID : CVE-2023-0912**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2023	8.8	A vulnerability classified as critical was found in SourceCodester Auto Dealer Management System 1.0. This vulnerability affects unknown code of the file /adms/admin/?page=vehicles/sell_vehicle. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221482 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0913**	N/A	A-AUT-AUTO-160323/88
Improper Neutralization of Special Elements used in an	19-Feb-2023	8.8	A vulnerability classified as critical has been found in SourceCodester Auto Dealer Management System 1.0. Affected	N/A	A-AUT-AUTO-160323/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			is an unknown function of the file /adms/admin/?page=user/manage_user. The manipulation of the argument 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-221490 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0915**		
N/A	19-Feb-2023	8.8	A vulnerability classified as critical was found in SourceCodester Auto Dealer Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /adms/classes/Users.php. The manipulation leads to improper access controls. 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-221491. **CVE ID : CVE-2023-0916**	N/A	A-AUT-AUTO-160323/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: axcora					
Product: axcora					
Affected Version(s): -					
N/A	21-Feb-2023	9.8	An access control issue in Axcora POS #0~gitf77ec09 allows unauthenticated attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2023-24320**	N/A	A-AXC-AXCO-160323/91
Vendor: best_pos_management_system_project					
Product: best_pos_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	A vulnerability has been found in SourceCodester Best POS Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file billing/index.php?id=9. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB-221593 was assigned to this vulnerability. **CVE ID : CVE-2023-0946**	N/A	A-BES-BEST-160323/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	21-Feb-2023	8.8	A vulnerability, which was classified as problematic, has been found in SourceCodester Best POS Management System 1.0. This issue affects some unknown processing of the file index.php?page=site_settings of the component Image Handler. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-221591. **CVE ID : CVE-2023-0943**	N/A	A-BES-BEST-160323/93
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	A vulnerability, which was classified as problematic, was found in SourceCodester Best POS Management System 1.0. Affected is an unknown function of the file index.php?page=add-category. The manipulation of the argument Name with the input "><img src=x onerror=prompt(document.domain);> leads to cross site scripting. It is	N/A	A-BES-BEST-160323/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to launch the attack remotely. The identifier of this vulnerability is VDB-221592. **CVE ID : CVE-2023-0945**		
Vendor: BMC					
Product: control-m					
Affected Version(s): * Up to (excluding) 9.0.20.214					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	9.8	A SQL injection vulnerability in BMC Control-M before 9.0.20.214 allows attackers to execute arbitrary SQL commands via the memname JSON field. **CVE ID : CVE-2023-26550**	N/A	A-BMC-CONT-160323/95
Vendor: bootstrapped					
Product: easy_affiliate_links					
Affected Version(s): * Up to (excluding) 3.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Easy Affiliate Links WordPress plugin before 3.7.1 does not validate and escape some of its block options before outputting them back in a page/post where the block is embedded, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	N/A	A-BOO-EASY-160323/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0375		
Vendor: borg_project					
Product: borg					
Affected Version(s): * Up to (excluding) 1.1.19					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Feb-2023	5.3	The Borg theme before 1.1.19 for Backdrop CMS does not sufficiently sanitize path arguments that are passed in via a URL. The function borg_preprocess_page in the file template.php does not properly sanitize incoming path arguments before using them. **CVE ID : CVE-2023-26265**	https://github.com/backdrop-contrib/borg/compare/1.x-1.1.18...1.x-1.1.19	A-BOR-BORG-160323/97
Vendor: bstek					
Product: urule					
Affected Version(s): 2.1.7					
Improper Restriction of XML External Entity Reference	24-Feb-2023	9.8	An XML External Entity (XXE) vulnerability in urule v2.1.7 allows attackers to execute arbitrary code via uploading a crafted XML file to /urule/common/saveFile. **CVE ID : CVE-2023-24189**	N/A	A-BST-URUL-160323/98
Vendor: btcpayserver					
Product: btcpay_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.7.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository btcpayserver/btcpayserver prior to 1.7.12. **CVE ID : CVE-2023-0879**	https://huntr.dev/bounties/9464e3c6-961d-4e23-8b3d-07cbb31de541, https://github.com/btcpayserver/btcpayserver/commit/f2f3b245c4d8980d8e54e4708c796df82332c3d7	A-BTC-BTCP-160323/99
Vendor: business_management_system_project					
Product: business_management_system					
Affected Version(s): * Up to (excluding) 2.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository unilogies/bumsys prior to v2.0.1. **CVE ID : CVE-2023-0995**	https://huntr.dev/bounties/2847b92b-22c2-4dbc-a9d9-56a7cd12fe5f, https://github.com/unilogies/bumsys/commit/927214bd7c475b31062c56294ff7b23d523a7219	A-BUS-BUSI-160323/100
Vendor: canteen_management_system_project					
Product: canteen_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an	17-Feb-2023	9.8	Canteen Management System 1.0 is vulnerable to SQL Injection via	N/A	A-CAN-CANT-160323/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			/php_action/getOrderReport.php. **CVE ID : CVE-2023-23279**		
Vendor: cellinx					
Product: nvt_web_server					
Affected Version(s): 1.0.6.002b					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Cellinx NVT v1.0.6.002b is vulnerable to local file disclosure. **CVE ID : CVE-2023-23063**	N/A	A-CEL-NVT_-160323/102
Vendor: cerebrate-project					
Product: cerebrate					
Affected Version(s): 1.12					
N/A	24-Feb-2023	9.1	Cerebrate 1.12 does not properly consider organisation_id during creation of API keys. **CVE ID : CVE-2023-26468**	https://github.com/cerebrate-project/cerebrate/commit/7ccf9252470a23acc38ad6ed13eecf523e368b48	A-CER-CERE-160323/103
Vendor: chamberlain					
Product: myq					
Affected Version(s): 5.222.0.32277					
Improper Restriction of Excessive Authentication Attempts	21-Feb-2023	9.8	A lack of rate limiting on the password reset endpoint of Chamberlain myQ v5.222.0.32277 (on iOS) allows attackers to compromise user	N/A	A-CHA-MYQ-160323/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accounts via a bruteforce attack. **CVE ID : CVE-2023-24080**		
Vendor: changedetection					
Product: changedetection					
Affected Version(s): * Up to (excluding) 0.40.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	5.4	Changedetection.io before v0.40.1.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the main page. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the URL parameter under the "Add a new change detection watch" function. **CVE ID : CVE-2023-24769**	https://github.com/dgtlmoon/changedetection.io/issues/1358	A-CHA-CHAN-160323/105
Vendor: checkoutplugins					
Product: stripe_payments_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.4.11					
Cross-Site Request Forgery (CSRF)	28-Feb-2023	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Checkout Plugins Stripe Payments For WooCommerce plugin <= 1.4.10 leads to settings change. **CVE ID : CVE-2023-23865**	N/A	A-CHE-STRI-160323/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Cisco					
Product: application_policy_infrastructure_controller					
Affected Version(s): From (including) 4.2\\(6\\) Up to (excluding) 5.2\\(7g\\)					
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the affected user has administrative privileges, these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-csrfv-DMx6KSwV	A-CIS-APPL-160323/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			actions could include modifying the system configuration and creating new privileged accounts. **CVE ID : CVE-2023-20011**		
Affected Version(s): From (including) 6.0 Up to (excluding) 6.0\\(2h\\)					
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-csrfv-DMx6KSwV	A-CIS-APPL-160323/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			level of the affected user. If the affected user has administrative privileges, these actions could include modifying the system configuration and creating new privileged accounts. **CVE ID : CVE-2023-20011**		
Product: cloud_network_controller					
Affected Version(s): From (including) 4.2\\(6\\) Up to (excluding) 25.0\\(5\\)					
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-csrfv-DMx6KSwV	A-CIS-CLOU-160323/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the affected user has administrative privileges, these actions could include modifying the system configuration and creating new privileged accounts. **CVE ID : CVE-2023-20011**		
Product: node-jose					
Affected Version(s): * Up to (excluding) 2.2.0					
Loop with Unreachable Exit Condition ('Infinite Loop')	16-Feb-2023	7.5	node-jose is a JavaScript implementation of the JSON Object Signing and Encryption (JOSE) for web browsers and node.js-based servers. Prior to version 2.2.0, when using the non-default "fallback" crypto back-end, ECC operations in `node-jose` can trigger a Denial-of-Service (DoS) condition, due to a possible infinite loop in an internal calculation. For some ECC operations, this condition is triggered randomly;	https://github.com/cisco/node-jose/commit/901d91508a70e3b9bdfc45688ea07bb4e1b8210d, https://github.com/cisco/node-jose/security/advisories/GHSA-5h4j-qrvg-9xhw	A-CIS-NODE-160323/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for others, it can be triggered by malicious input. The issue has been patched in version 2.2.0. Since this issue is only present in the "fallback" crypto implementation, it can be avoided by ensuring that either WebCrypto or the Node `crypto` module is available in the JS environment where `node-jose` is being run. **CVE ID : CVE-2023-25653**		
Product: ucs_central_software					
Affected Version(s): * Up to (excluding) 4.2\\(3c\\)					
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	A-CIS-UCS_-160323/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Affected Version(s): From (including) 4.0 Up to (excluding) 4.0\\(4o\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	A-CIS-UCS_-160323/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Affected Version(s): From (including) 4.1 Up to (excluding) 4.1\\(3k\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	A-CIS-UCS_-160323/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Affected Version(s): From (including) 4.2 Up to (excluding) 4.2\\(2d\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	A-CIS-UCS_-160323/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	A-CIS-UCS_-160323/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**	o-sa-elyfex-dos-gfvcByx	
Vendor: Citrix					
Product: virtual_apps_and_desktops					
Affected Version(s): * Up to (excluding) 2212					
Improper Privilege Management	16-Feb-2023	7.8	A vulnerability has been identified that, if exploited, could result in a local user elevating their privilege level to NT	https://support.citrix.com/article/CTX477616/citrix-virtual-apps-and-desktops-	A-CIT-VIRT-160323/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AUTHORITY\SYSTEM on a Citrix Virtual Apps and Desktops Windows VDA. **CVE ID : CVE-2023-24483**	security-bulletin-for-cve202324483	
Affected Version(s): 1912					
Improper Privilege Management	16-Feb-2023	7.8	A vulnerability has been identified that, if exploited, could result in a local user elevating their privilege level to NT AUTHORITY\SYSTEM on a Citrix Virtual Apps and Desktops Windows VDA. **CVE ID : CVE-2023-24483**	https://support.citrix.com/article/CTX477616/citrix-virtual-apps-and-desktops-security-bulletin-for-cve202324483	A-CIT-VIRT-160323/117
Affected Version(s): 2203					
Improper Privilege Management	16-Feb-2023	7.8	A vulnerability has been identified that, if exploited, could result in a local user elevating their privilege level to NT AUTHORITY\SYSTEM on a Citrix Virtual Apps and Desktops Windows VDA. **CVE ID : CVE-2023-24483**	https://support.citrix.com/article/CTX477616/citrix-virtual-apps-and-desktops-security-bulletin-for-cve202324483	A-CIT-VIRT-160323/118
Product: workspace					
Affected Version(s): * Up to (excluding) 2212					
Incorrect Authorization	16-Feb-2023	7.8	Vulnerabilities have been identified that, collectively, allow a standard Windows user to perform operations as SYSTEM on the	https://support.citrix.com/article/CTX477617/citrix-workspace-app-for-windows-	A-CIT-WORK-160323/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			computer running Citrix Workspace app. **CVE ID : CVE-2023-24485**	security-bulletin-for-cve20232448 4-cve20232448 5	
N/A	16-Feb-2023	5.5	A malicious user can cause log files to be written to a directory that they do not have permission to write to. **CVE ID : CVE-2023-24484**	https://support.citrix.com/article/CTX477617/citrix-workspace-app-for-windows-security-bulletin-for-cve20232448 4-cve20232448 5	A-CIT-WORK-160323/120
Affected Version(s): 1912					
Incorrect Authorization	16-Feb-2023	7.8	Vulnerabilities have been identified that, collectively, allow a standard Windows user to perform operations as SYSTEM on the computer running Citrix Workspace app. **CVE ID : CVE-2023-24485**	https://support.citrix.com/article/CTX477617/citrix-workspace-app-for-windows-security-bulletin-for-cve20232448 4-cve20232448 5	A-CIT-WORK-160323/121
N/A	16-Feb-2023	5.5	A malicious user can cause log files to be written to a directory that they do not have permission to write to. **CVE ID : CVE-2023-24484**	https://support.citrix.com/article/CTX477617/citrix-workspace-app-for-windows-security-bulletin-for-cve20232448	A-CIT-WORK-160323/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				4-cve202324485	
Affected Version(s): 2203.1					
Incorrect Authorization	16-Feb-2023	7.8	Vulnerabilities have been identified that, collectively, allow a standard Windows user to perform operations as SYSTEM on the computer running Citrix Workspace app. **CVE ID : CVE-2023-24485**	https://support.citrix.com/article/CTX477617/citrix-workspace-app-for-windows-security-bulletin-for-cve202324484-cve202324485	A-CIT-WORK-160323/123
N/A	16-Feb-2023	5.5	A malicious user can cause log files to be written to a directory that they do not have permission to write to. **CVE ID : CVE-2023-24484**	https://support.citrix.com/article/CTX477617/citrix-workspace-app-for-windows-security-bulletin-for-cve202324484-cve202324485	A-CIT-WORK-160323/124
Vendor: clash_project					
Product: clash					
Affected Version(s): 0.20.12					
Incorrect Permission Assignment for Critical Resource	23-Feb-2023	9.8	Clash for Windows v0.20.12 was discovered to contain a remote code execution (RCE) vulnerability which is exploited via overwriting the	N/A	A-CLA-CLAS-160323/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration file (cfw-setting.yaml). **CVE ID : CVE-2023-24205**		
Vendor: class_and_exam_timetabling_system_project					
Product: class_and_exam_timetabling_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Feb-2023	8.8	A vulnerability classified as critical was found in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/index3.php of the component POST Parameter Handler. The manipulation of the argument password leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221797 was assigned to this vulnerability. **CVE ID : CVE-2023-1039**	N/A	A-CLA-CLAS-160323/126
Vendor: clinics_patient_management_system_project					
Product: clinics_patient_management_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	8.8	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been classified as critical. Affected is an unknown function of the file update_user.php. The manipulation of the argument user_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. The identifier of this vulnerability is VDB-221784. **CVE ID : CVE-2023-1035**	N/A	A-CLI-CLIN-160323/127
Vendor: correos					
Product: correos_oficial					
Affected Version(s): * Up to (including) 1.2.0.2					
Files or Directories Accessible to External Parties	27-Feb-2023	7.5	The Correos Oficial WordPress plugin through 1.2.0.2 does not have an authorization check user input validation when generating a file path, allowing unauthenticated attackers to download arbitrary files from the server. **CVE ID : CVE-2023-0331**	N/A	A-COR-CORR-160323/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: covesa					
Product: dlt-daemon					
Affected Version(s): * Up to (including) 2.18.8					
Missing Release of Memory after Effective Lifetime	27-Feb-2023	7.5	An issue was discovered in the Connected Vehicle Systems Alliance (COVESA; formerly GENIVI) dlt-daemon through 2.18.8. Dynamic memory is not released after it is allocated in dlt-control-common.c. **CVE ID : CVE-2023-26257**	https://github.com/COVESA/dlt-daemon/pull/441/commits/b6149e203f919c899fefc702a17fbb78bdec3700	A-COV-DLT--160323/129
Vendor: Craftercms					
Product: crafter_cms					
Affected Version(s): From (including) 3.1.0 Up to (including) 3.1.26					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26. **CVE ID : CVE-2023-26020**	https://docs.craftercms.org/en/4.0/security/advisory.html#cv-2023021701	A-CRA-CRAF-160323/130
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26. **CVE ID : CVE-2023-26020**	https://docs.craftercms.org/en/4.0/security/advisory.html#cv-2023021701	A-CRA-CRAF-160323/131
Vendor: crasm_project					
Product: crasm					
Affected Version(s): 1.8-3					
NULL Pointer Dereference	27-Feb-2023	7.5	In crasm 1.8-3, invalid input validation, specific files passed to the command line application, can lead to a NULL pointer dereference in the function Xasc. **CVE ID : CVE-2023-23108**	https://github.com/colinbourassa/crasm/pull/7	A-CRA-CRAS-160323/132
Divide By Zero	27-Feb-2023	7.5	In crasm 1.8-3, invalid input validation, specific files passed to the command line application, can lead to a divide by zero	https://github.com/colinbourassa/crasm/pull/7	A-CRA-CRAS-160323/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fault in the function opdiv. **CVE ID : CVE-2023-23109**		
Vendor: dataease					
Product: dataease					
Affected Version(s): * Up to (excluding) 1.18.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Feb-2023	5.4	DataEase is an open source data visualization and analysis tool. When saving a dashboard on the DataEase platform saved data can be modified and store malicious code. This vulnerability can lead to the execution of malicious code stored by the attacker on the server side when the user accesses the dashboard. The vulnerability has been fixed in version 1.18.3. **CVE ID : CVE-2023-25807**	https://github.com/dataease/dataease/commit/cc94fb8e69ddbb37c96d02ec0f0ddcd74273ef49, https://github.com/dataease/dataease/security/advisories/GHSA-xj3h-3wmw-j5vf	A-DAT-DATA-160323/134
Vendor: davinci_project					
Product: davinci					
Affected Version(s): 0.3.0					
Improper Neutralization of Special Elements used in an SQL Command	27-Feb-2023	9.8	Davinci v0.3.0-rc was discovered to contain a SQL injection vulnerability via the copyDisplay function.	N/A	A-DAV-DAVI-160323/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2023-24206**		
Vendor: Dell					
Product: multifunction_printer_e525w_driver_and_software_suite					
Affected Version(s): * Up to (excluding) 1.047.2022\\,_a05					
N/A	21-Feb-2023	7.8	Dell Multifunction Printer E525w Driver and Software Suite, versions prior to 1.047.2022, A05, contain a local privilege escalation vulnerability that could be exploited by malicious users to compromise the affected system **CVE ID : CVE-2023-24575**	https://www.dell.com/support/kbdoc/en-us/000208396/dsa-2023-043	A-DEL-MULT-160323/136
Product: secure_connect_gateway					
Affected Version(s): 5.12.00.10					
Use of a Broken or Risky Cryptographic Algorithm	17-Feb-2023	5.9	Dell Secure Connect Gateway (SCG) version 5.14.00.12 contains a broken cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by performing MitM attacks and let attackers obtain sensitive information. **CVE ID : CVE-2023-23695**	https://www.dell.com/support/kbdoc/en-us/000208462/dsa-2023-020-dell-secure-connect-gateway-security-update-for-multiple-vulnerabilities	A-DEL-SECU-160323/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 5.14.00.12					
Use of a Broken or Risky Cryptographic Algorithm	17-Feb-2023	5.9	Dell Secure Connect Gateway (SCG) version 5.14.00.12 contains a broken cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by performing MitM attacks and let attackers obtain sensitive information. **CVE ID : CVE-2023-23695**	https://www.dell.com/support/kbdoc/en-us/000208462/dsa-2023-020-dell-secure-connect-gateway-security-update-for-multiple-vulnerabilities	A-DEL-SECU-160323/138
Vendor: deltaww					
Product: diaenergie					
Affected Version(s): * Up to (excluding) 1.9.03.001					
Files or Directories Accessible to External Parties	17-Feb-2023	8.8	The affected product DIAEnergie (versions prior to v1.9.03.001) contains improper authorization, which could allow an unauthorized user to bypass authorization and access privileged functionality. **CVE ID : CVE-2023-0822**	N/A	A-DEL-DIAE-160323/139
Vendor: deno					
Product: deno					
Affected Version(s): * Up to (excluding) 1.31.0					
N/A	25-Feb-2023	7.5	Versions of the package deno before	https://github.com/denolan	A-DEN-DENO-160323/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.31.0 are vulnerable to Regular Expression Denial of Service (ReDoS) due to the upgradeWebSocket function, which contains regexes in the form of /s*,s*/, used for splitting the Connection/Upgrade header. A specially crafted Connection/Upgrade header can be used to significantly slow down a web socket server. **CVE ID : CVE-2023-26103**	d/deno/pull/17722, https://github.com/denoland/deno/commit/cf06a7c7e672880e1b38598fe445e2c50b4a9d06	
Vendor: dental_clinic_appointment_reservation_system_project					
Product: dental_clinic_appointment_reservation_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Feb-2023	9.8	A vulnerability was found in SourceCodester Dental Clinic Appointment Reservation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /APR/login.php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. The attack may be	N/A	A-DEN-DENT-160323/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221795. **CVE ID : CVE-2023-1037**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Feb-2023	6.1	A vulnerability was found in SourceCodester Dental Clinic Appointment Reservation System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /APR/signup.php of the component POST Parameter Handler. The manipulation of the argument firstname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221794 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1036**	N/A	A-DEN-DENT-160323/142
Vendor: devowl					
Product: real_media_library					
Affected Version(s): * Up to (excluding) 4.18.29					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Real Media Library WordPress plugin before 4.18.29 does not sanitise and escape the created folder names, which could allow users with the role of author and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0285**	N/A	A-DEV-REAL-160323/143
Vendor: docmosis					
Product: tornado					
Affected Version(s): * Up to (excluding) 2.9.5					
N/A	28-Feb-2023	8.8	An issue was discovered in Docmosis Tornado prior to version 2.9.5. An authenticated attacker can change the Office directory setting pointing to an arbitrary remote network path. This triggers the execution of the soffice binary under the attackers control leading to arbitrary remote code execution (RCE). **CVE ID : CVE-2023-25266**	N/A	A-DOC-TORN-160323/144
Improper Authentication	28-Feb-2023	7.5	An issue was discovered in Docmosis Tornado prior to version 2.9.5. An	N/A	A-DOC-TORN-160323/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker can bypass the authentication check filter completely by introducing a specially crafted request with relative path segments. **CVE ID : CVE-2023-25264**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.5	Docmosis Tornado <= 2.9.4 is vulnerable to Directory Traversal leading to the disclosure of arbitrary content on the file system. **CVE ID : CVE-2023-25265**	N/A	A-DOC-TORN-160323/146
Vendor: doctors_appointment_system_project					
Product: doctors_appointment_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /edoc/doctor/patient.php. The manipulation of the argument search12 leads to sql injection. The attack can be launched remotely.	N/A	A-DOC-DOCT-160323/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The identifier VDB-221821 was assigned to this vulnerability. **CVE ID : CVE-2023-1056**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been rated as critical. Affected by this issue is the function edoc of the file login.php. The manipulation of the argument usermail leads to sql injection. VDB-221822 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1057**	N/A	A-DOC-DOCT-160323/148
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability classified as critical has been found in SourceCodester Doctors Appointment System 1.0. This affects an unknown part of the file create-account.php. The manipulation of the argument newemail leads to sql injection. It is possible to initiate the attack remotely. The exploit	N/A	A-DOC-DOCT-160323/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221823. **CVE ID : CVE-2023-1058**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability classified as critical was found in SourceCodester Doctors Appointment System 1.0. This vulnerability affects unknown code of the file /admin/doctors.php of the component Parameter Handler. The manipulation of the argument search 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-221824. **CVE ID : CVE-2023-1059**	N/A	A-DOC-DOCT-160323/150
Improper Neutralization of Special Elements used in an SQL Command	27-Feb-2023	8.8	A vulnerability, which was classified as critical, has been found in SourceCodester Doctors Appointment System 1.0. This issue affects some unknown	N/A	A-DOC-DOCT-160323/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			processing of the file /admin/edit-doc.php. The manipulation of the argument oldmail 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-221825 was assigned to this vulnerability. **CVE ID : CVE-2023-1061**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability, which was classified as critical, was found in SourceCodester Doctors Appointment System 1.0. Affected is an unknown function of the file /admin/add-new.php of the component Parameter Handler. The manipulation of the argument email 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-221826 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1062**	N/A	A-DOC-DOCT-160323/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	A vulnerability has been found in SourceCodester Doctors Appointment System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/patient.php of the component Parameter Handler. The manipulation of the argument search leads to sql injection. 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-221827. **CVE ID : CVE-2023-1063**	N/A	A-DOC-DOCT-160323/153
Vendor: dolphinphp_project					
Product: dolphinphp					
Affected Version(s): * Up to (including) 1.5.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Feb-2023	9.8	A vulnerability was found in DolphinPHP up to 1.5.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file common.php of the component Incomplete Fix CVE-	N/A	A-DOL-DOLP-160323/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2021-46097. The manipulation of the argument id leads to os command injection. 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-221551. **CVE ID : CVE-2023-0935**		
Vendor: domoticalabs					
Product: ikon_server					
Affected Version(s): * Up to (excluding) 2.8.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	9.8	Domotica Labs srl Ikon Server before v2.8.6 was discovered to contain a SQL injection vulnerability. **CVE ID : CVE-2023-24253**	N/A	A-DOM-IKON-160323/155
Vendor: donation_block_for_paypal_project					
Product: donation_block_for_paypal					
Affected Version(s): * Up to (excluding) 2.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	The Donation Block For PayPal WordPress plugin before 2.1.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode	N/A	A-DON-DONA-160323/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0535**		
Vendor: ecisp					
Product: espcms					
Affected Version(s): p8.21120101					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	An issue was discovered in ESPCMS P8.21120101 after logging in to the background, there is a SQL injection vulnerability in the function node where members are added. **CVE ID : CVE-2023-23007**	N/A	A-ECI-ESPC-160323/157
Vendor: embedsocial					
Product: embedsocial					
Affected Version(s): * Up to (excluding) 1.1.28					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The EmbedSocial WordPress plugin before 1.1.28 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	N/A	A-EMB-EMBE-160323/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0371**		
Product: embedstories					
Affected Version(s): * Up to (excluding) 0.7.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The EmbedStories WordPress plugin before 0.7.5 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-2023-0372**	N/A	A-EMB-EMBE-160323/159
Vendor: employee_task_management_system_project					
Product: employee_task_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2023	8.8	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file edit-task.php. The manipulation of the argument task_id leads to sql injection.	N/A	A-EMP-EMPL-160323/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-221452. **CVE ID : CVE-2023-0903**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Feb-2023	8.8	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file task-details.php. The manipulation of the argument task_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-221453 was assigned to this vulnerability. **CVE ID : CVE-2023-0904**	N/A	A-EMP-EMPL-160323/161
Improper Authentication	18-Feb-2023	7.5	A vulnerability classified as critical has been found in SourceCodester Employee Task Management System 1.0. Affected is an unknown function of	N/A	A-EMP-EMPL-160323/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file changePasswordForEmployee.php. The manipulation leads to improper authentication. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-221454 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0905**		
Vendor: eternal_terminal_project					
Product: eternal_terminal					
Affected Version(s): 6.2.1					
Improper Link Resolution Before File Access ('Link Following')	16-Feb-2023	6.3	In Eternal Terminal 6.2.1, TelemetryService uses fixed paths in /tmp. For example, a local attacker can create /tmp/.sentry-native-etserver with mode 0777 before the etserver process is started. The attacker can choose to read sensitive information from that file, or modify the information in that file. **CVE ID : CVE-2023-23558**	http://www.openwall.com/lists/oss-security/2023/02/16/1	A-ETE-ETER-160323/163
Vendor: executablebooks					
Product: markdown-it-py					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.2.0					
N/A	22-Feb-2023	5.5	Denial of service could be caused to the command line interface of markdown-it-py, before v2.2.0, if an attacker was allowed to use invalid UTF-8 characters as input. **CVE ID : CVE-2023-26302**	https://github.com/executablebooks/markdown-it-py/commit/53ca3e9c2b9e9b295f6abf7f4ad2730a9b70f68c	A-EXE-MARK-160323/164
N/A	23-Feb-2023	5.5	Denial of service could be caused to markdown-it-py, before v2.2.0, if an attacker was allowed to force null assertions with specially crafted input. **CVE ID : CVE-2023-26303**	https://github.com/executablebooks/markdown-it-py/commit/ae03c6107dfa18e648f6fdd1280f5b89092d5d49	A-EXE-MARK-160323/165
Vendor: Filseclab					
Product: twister_antivirus					
Affected Version(s): 8.17					
Improper Access Control	24-Feb-2023	7.8	A vulnerability was found in Twister Antivirus 8.17. It has been declared as critical. This vulnerability affects unknown code in the library filmfd.sys of the component IoControlCode Handler. The manipulation leads to improper access controls. The attack needs to be	https://github.com/zeze-zeze/WindowsKernelVuln/tree/master/CVE-2023-1007	A-FIL-TWIS-160323/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221740. **CVE ID : CVE-2023-1007**		
Improper Resource Shutdown or Release	18-Feb-2023	5.5	A vulnerability, which was classified as problematic, has been found in Filseclab Twister Antivirus 8.17. Affected by this issue is some unknown functionality in the library ffsmon.sys of the component IoControlCode Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221456. **CVE ID : CVE-2023-0907**	N/A	A-FIL-TWIS-160323/167
Improper Resource Shutdown or Release	24-Feb-2023	5.5	A vulnerability was found in Twister Antivirus 8.17. It has been rated as problematic. This issue affects some unknown processing in the library filmfd.sys of the	https://github.com/zeze-zeze/WindowsKernelVuln/tree/master/CVE-2023-1008	A-FIL-TWIS-160323/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component IoControlCode Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-221741 was assigned to this vulnerability. **CVE ID : CVE-2023-1008**		
Vendor: Flatpress					
Product: flatpress					
Affected Version(s): * Up to (including) 1.2.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	9.8	Path Traversal in GitHub repository flatpressblog/flatpress prior to 1.3. **CVE ID : CVE-2023-0947**	https://huntr.dev/bounties/7379d702-72ff-4a5d-bc68-007290015496, https://github.com/flatpressblog/flatpress/commit/9c4e5d6567e446c472f3adae3b2fe612f66871c7	A-FLA-FLAT-160323/169
Vendor: Forgerock					
Product: java_policy_agents					
Affected Version(s): * Up to (including) 5.10.1					
Improper Limitation of a Pathname	28-Feb-2023	9.8	Relative Path Traversal vulnerability in ForgeRock Access	https://backstage.forgerock.com/knowled	A-FOR-JAVA-160323/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Management Java Policy Agent allows Authentication Bypass. This issue affects Access Management Java Policy Agent: all versions up to 5.10.1 **CVE ID : CVE-2023-0511**	ge/kb/article/a21576868	
Product: web_policy_agents					
Affected Version(s): * Up to (including) 5.10.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	9.8	Relative Path Traversal vulnerability in ForgeRock Access Management Web Policy Agent allows Authentication Bypass. This issue affects Access Management Web Policy Agent: all versions up to 5.10.1 **CVE ID : CVE-2023-0339**	https://backstage.forgerock.com/knowledge/kb/article/a21576868	A-FOR-WEB_-160323/171
Vendor: Fortinet					
Product: fortinac					
Affected Version(s): 8.3.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and	https://fortiguard.com/psirt/FG-IR-22-260	A-FOR-FORT-160323/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. **CVE ID : CVE-2023-22638**		
Affected Version(s): 9.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. **CVE ID : CVE-2023-22638**	https://fortiguard.com/psirt/FG-IR-22-260	A-FOR-FORT-160323/173
Affected Version(s): 9.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and	https://fortiguard.com/psirt/FG-IR-22-260	A-FOR-FORT-160323/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. **CVE ID : CVE-2023-22638**		
Affected Version(s): From (including) 8.5.0 Up to (including) 8.5.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. **CVE ID : CVE-2023-22638**	https://fortiguard.com/psirt/FG-IR-22-260	A-FOR-FORT-160323/175
Affected Version(s): From (including) 8.6.0 Up to (including) 8.6.5					
Improper Neutralization of Input During Web Page Generation	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and	https://fortiguard.com/psirt/FG-IR-22-260	A-FOR-FORT-160323/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. **CVE ID : CVE-2023-22638**		
Affected Version(s): From (including) 8.7.0 Up to (including) 8.7.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. **CVE ID : CVE-2023-22638**	https://fortiguard.com/psirt/FG-IR-22-260	A-FOR-FORT-160323/177
Affected Version(s): From (including) 8.8.0 Up to (including) 8.8.11					
Improper Neutralization of Input During Web Page	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC 9.4.1	https://fortiguard.com/psirt/FG-IR-22-260	A-FOR-FORT-160323/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. **CVE ID : CVE-2023-22638**		
Affected Version(s): From (including) 9.1.0 Up to (including) 9.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation vulnerability [CWE-79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. **CVE ID : CVE-2023-22638**	https://fortiguard.com/psirt/FG-IR-22-260	A-FOR-FORT-160323/179
Affected Version(s): From (including) 9.2.0 Up to (including) 9.2.7					
Improper Neutralization of Input	16-Feb-2023	5.4	Several improper neutralization of inputs during web page generation	https://fortiguard.com/psirt/FG-IR-22-260	A-FOR-FORT-160323/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability [CWE-79] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below, 8.6.5 and below, 8.5.4 and below, 8.3.7 and below may allow an authenticated attacker to perform several XSS attacks via crafted HTTP GET requests. **CVE ID : CVE-2023-22638**		
Product: fortiweb					
Affected Version(s): 6.4.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. **CVE ID : CVE-2023-23779**	N/A	A-FOR-FORT-160323/181
Improper Limitation	16-Feb-2023	6.5	A relative path traversal	https://fortiguard.com/psir	A-FOR-FORT-160323/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			vulnerability [CWE-23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests. **CVE ID : CVE-2023-23778**	t/FG-IR-22-142	
Affected Version(s): 6.4.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. **CVE ID : CVE-2023-23779**	N/A	A-FOR-FORT-160323/183
Improper Limitation of a Pathname to a	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE-23] in FortiWeb version 7.0.1 and	https://fortiguard.com/psirt/FG-IR-22-142	A-FOR-FORT-160323/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests. **CVE ID : CVE-2023-23778**		
Affected Version(s): 6.4.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. **CVE ID : CVE-2023-23779**	N/A	A-FOR-FORT-160323/185
Improper Limitation of a Pathname to a Restricted Directory	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE-23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.2 all	https://fortiguard.com/psirt/FG-IR-22-142	A-FOR-FORT-160323/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests. **CVE ID : CVE-2023-23778**		
Affected Version(s): 7.0.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. **CVE ID : CVE-2023-23779**	N/A	A-FOR-FORT-160323/187
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE-23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain	https://fortiguard.com/psirt/FG-IR-22-142	A-FOR-FORT-160323/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to files and data via specifically crafted web requests. **CVE ID : CVE-2023-23778**		
Affected Version(s): 7.0.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. **CVE ID : CVE-2023-23779**	N/A	A-FOR-FORT-160323/189
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE-23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via	https://fortiguard.com/psirt/FG-IR-22-142	A-FOR-FORT-160323/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted web requests. **CVE ID : CVE-2023-23778**		
Affected Version(s): From (including) 5.6.0 Up to (excluding) 5.9.2					
Out-of-bounds Write	16-Feb-2023	7.8	A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2023-25602**	https://fortiguard.com/psirt/FG-IR-21-234	A-FOR-FORT-160323/191
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.8					
Out-of-bounds Write	16-Feb-2023	7.8	A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and	https://fortiguard.com/psirt/FG-IR-21-234	A-FOR-FORT-160323/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2023-25602**		
Affected Version(s): From (including) 6.0.0 Up to (including) 6.2.7					
Out-of-bounds Write	16-Feb-2023	7.8	A heap-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb version 6.3.0 through 6.3.19, FortiWeb 6.4 all versions, FortiWeb 6.2 all versions, FortiWeb 6.1 all versions allows attacker to escalation of privilege via specifically crafted arguments to existing commands. **CVE ID : CVE-2023-23782**	https://fortiguard.com/psirt/FG-IR-22-111	A-FOR-FORT-160323/193
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.3					
Out-of-bounds Write	16-Feb-2023	7.8	A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb	https://fortiguard.com/psirt/FG-IR-21-234	A-FOR-FORT-160323/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2023-25602**		
Affected Version(s): From (including) 6.2.0 Up to (excluding) 6.2.7					
Out-of-bounds Write	16-Feb-2023	7.8	A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to	https://fortiguard.com/psirt/FG-IR-21-234	A-FOR-FORT-160323/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2023-25602**		
Affected Version(s): From (including) 6.2.3 Up to (including) 6.2.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE-23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests. **CVE ID : CVE-2023-23778**	https://fortiguard.com/psirt/FG-IR-22-142	A-FOR-FORT-160323/196
Affected Version(s): From (including) 6.3.0 Up to (excluding) 6.3.18					
Out-of-bounds Write	16-Feb-2023	7.8	A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions,	https://fortiguard.com/psirt/FG-IR-21-234	A-FOR-FORT-160323/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2023-25602**		
Affected Version(s): From (including) 6.3.0 Up to (excluding) 6.3.20					
Out-of-bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, Fortinet FortiWeb version 6.3.6 through 6.3.19, Fortinet FortiWeb 6.4 all versions allows attacker to escalation of privilege via specifically crafted HTTP requests. **CVE ID : CVE-2023-23780**	https://fortiguard.com/psirt/FG-IR-22-118	A-FOR-FORT-160323/198
Out-of-bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow vulnerability [CWE-121] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below SAML server configuration may allow an authenticated attacker to achieve	https://fortiguard.com/psirt/FG-IR-22-151	A-FOR-FORT-160323/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution via specifically crafted XML files. **CVE ID : CVE-2023-23781**		
Out-of-bounds Write	16-Feb-2023	7.8	A heap-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb version 6.3.0 through 6.3.19, FortiWeb 6.4 all versions, FortiWeb 6.2 all versions, FortiWeb 6.1 all versions allows attacker to escalation of privilege via specifically crafted arguments to existing commands. **CVE ID : CVE-2023-23782**	https://fortiguard.com/psirt/FG-IR-22-111	A-FOR-FORT-160323/200
Affected Version(s): From (including) 6.3.0 Up to (including) 6.3.21					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal vulnerability [CWE-23] in FortiWeb version 7.0.1 and below, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated user to obtain unauthorized access to files and data via specifically crafted web requests. **CVE ID : CVE-2023-23778**	https://fortiguard.com/psirt/FG-IR-22-142	A-FOR-FORT-160323/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 6.3.6 Up to (excluding) 6.3.21					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal in Fortinet FortiWeb version 7.0.0 through 7.0.2, FortiWeb version 6.3.6 through 6.3.20, FortiWeb 6.4 all versions allows attacker to information disclosure via specially crafted web requests. **CVE ID : CVE-2023-23784**	https://fortiguard.com/psirt/FG-IR-22-251	A-FOR-FORT-160323/202
Affected Version(s): From (including) 6.3.6 Up to (including) 6.3.19					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	Multiple improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerabilities [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below may allow an authenticated attacker to execute unauthorized code or commands via crafted parameters of HTTP requests. **CVE ID : CVE-2023-23779**	N/A	A-FOR-FORT-160323/203
Affected Version(s): From (including) 6.3.6 Up to (including) 6.3.21					
N/A	27-Feb-2023	3.3	An unauthorized configuration download	https://fortiguard.com/psir	A-FOR-FORT-160323/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in FortiWeb 6.3.6 through 6.3.21, 6.4.0 through 6.4.2 and 7.0.0 through 7.0.4 may allow a local attacker to access confidential configuration files via a crafted http request. **CVE ID : CVE-2023-22636**	t/FG-IR-22-460	
Affected Version(s): From (including) 6.4.0 Up to (excluding) 6.4.2					
Use of Externally-Controlled Format String	16-Feb-2023	7.8	A use of externally-controlled format string in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb 6.4 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2023-23783**	https://fortiguard.com/psirt/FG-IR-22-187	A-FOR-FORT-160323/205
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.2					
Out-of-bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, Fortinet FortiWeb version 6.3.6 through 6.3.19, Fortinet FortiWeb 6.4 all versions allows attacker to escalation of privilege via	https://fortiguard.com/psirt/FG-IR-22-118	A-FOR-FORT-160323/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted HTTP requests. **CVE ID : CVE-2023-23780**		
Out-of-bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow vulnerability [CWE-121] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below SAML server configuration may allow an authenticated attacker to achieve arbitrary code execution via specifically crafted XML files. **CVE ID : CVE-2023-23781**	https://fortiguard.com/psirt/FG-IR-22-151	A-FOR-FORT-160323/207
Out-of-bounds Write	16-Feb-2023	7.8	A heap-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb version 6.3.0 through 6.3.19, FortiWeb 6.4 all versions, FortiWeb 6.2 all versions, FortiWeb 6.1 all versions allows attacker to escalation of privilege via specifically crafted arguments to existing commands. **CVE ID : CVE-2023-23782**	https://fortiguard.com/psirt/FG-IR-22-111	A-FOR-FORT-160323/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Feb-2023	7.8	A stack-based buffer overflow in Fortinet FortiWeb 6.4 all versions, FortiWeb versions 6.3.17 and earlier, FortiWeb versions 6.2.6 and earlier, FortiWeb versions 6.1.2 and earlier, FortiWeb versions 6.0.7 and earlier, FortiWeb versions 5.9.1 and earlier, FortiWeb 5.8 all versions, FortiWeb 5.7 all versions, FortiWeb 5.6 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2023-25602**	https://fortiguard.com/psirt/FG-IR-21-234	A-FOR-FORT-160323/209
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal in Fortinet FortiWeb version 7.0.0 through 7.0.2, FortiWeb version 6.3.6 through 6.3.20, FortiWeb 6.4 all versions allows attacker to information disclosure via specially crafted web requests. **CVE ID : CVE-2023-23784**	https://fortiguard.com/psirt/FG-IR-22-251	A-FOR-FORT-160323/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Feb-2023	3.3	An unauthorized configuration download vulnerability in FortiWeb 6.3.6 through 6.3.21, 6.4.0 through 6.4.2 and 7.0.0 through 7.0.4 may allow a local attacker to access confidential configuration files via a crafted http request. **CVE ID : CVE-2023-22636**	https://fortiguard.com/psirt/FG-IR-22-460	A-FOR-FORT-160323/211
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.2					
Out-of-bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, Fortinet FortiWeb version 6.3.6 through 6.3.19, Fortinet FortiWeb 6.4 all versions allows attacker to escalation of privilege via specifically crafted HTTP requests. **CVE ID : CVE-2023-23780**	https://fortiguard.com/psirt/FG-IR-22-118	A-FOR-FORT-160323/212
Out-of-bounds Write	16-Feb-2023	8.8	A stack-based buffer overflow vulnerability [CWE-121] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.19 and below SAML server	https://fortiguard.com/psirt/FG-IR-22-151	A-FOR-FORT-160323/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration may allow an authenticated attacker to achieve arbitrary code execution via specifically crafted XML files. **CVE ID : CVE-2023-23781**		
Out-of-bounds Write	16-Feb-2023	7.8	A heap-based buffer overflow in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb version 6.3.0 through 6.3.19, FortiWeb 6.4 all versions, FortiWeb 6.2 all versions, FortiWeb 6.1 all versions allows attacker to escalation of privilege via specifically crafted arguments to existing commands. **CVE ID : CVE-2023-23782**	https://fortiguard.com/psirt/FG-IR-22-111	A-FOR-FORT-160323/214
Use of Externally-Controlled Format String	16-Feb-2023	7.8	A use of externally-controlled format string in Fortinet FortiWeb version 7.0.0 through 7.0.1, FortiWeb 6.4 all versions allows attacker to execute unauthorized code or commands via specially crafted command arguments.	https://fortiguard.com/psirt/FG-IR-22-187	A-FOR-FORT-160323/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23783		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A relative path traversal in Fortinet FortiWeb version 7.0.0 through 7.0.2, FortiWeb version 6.3.6 through 6.3.20, FortiWeb 6.4 all versions allows attacker to information disclosure via specially crafted web requests. **CVE ID : CVE-2023-23784**	https://fortiguard.com/psirt/FG-IR-22-251	A-FOR-FORT-160323/216
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.4					
N/A	27-Feb-2023	3.3	An unauthorized configuration download vulnerability in FortiWeb 6.3.6 through 6.3.21, 6.4.0 through 6.4.2 and 7.0.0 through 7.0.4 may allow a local attacker to access confidential configuration files via a crafted http request. **CVE ID : CVE-2023-22636**	https://fortiguard.com/psirt/FG-IR-22-460	A-FOR-FORT-160323/217
Vendor: frappant					
Product: forms_export					
Affected Version(s): * Up to (excluding) 3.1.2					
Improper Neutralization of	26-Feb-2023	6.1	The frp_form_answers (aka Forms Export)	https://typo3.org/security/advisory/typo	A-FRA-FORM-160323/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			extension before 3.1.2, and 4.x before 4.0.2, for TYPO3 allows XSS via saved emails. **CVE ID : CVE-2023-26091**	3-ext-sa-2023-002, https://typo3.org/help/security-advisories	
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Feb-2023	6.1	The frp_form_answers (aka Forms Export) extension before 3.1.2, and 4.x before 4.0.2, for TYPO3 allows XSS via saved emails. **CVE ID : CVE-2023-26091**	https://typo3.org/security/advisory/typo3-ext-sa-2023-002, https://typo3.org/help/security-advisories	A-FRA-FORM-160323/219
Vendor: Froxlor					
Product: froxlor					
Affected Version(s): * Up to (excluding) 2.0.11					
Improper Control of Generation of Code ('Code Injection')	17-Feb-2023	8.8	Code Injection in GitHub repository froxlor/froxlor prior to 2.0.11. **CVE ID : CVE-2023-0877**	https://huntr.dev/bounties/b29cf038-06f1-4fb0-9437-08f2991f92a8, https://github.com/froxlor/froxlor/commit/aa48ffca2bcaf7ae57be3b8147bb3138abdab984	A-FRO-FROX-160323/220
Cross-Site Request Forgery (CSRF)	25-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) in GitHub repository froxlor/froxlor prior to 2.0.11.	https://huntr.dev/bounties/ba3cd929-8b60-4d8d-b77d-f28409ecf387,	A-FRO-FROX-160323/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1033	https://github.com/froxlor/froxlor/commit/4003a8d2b60728a77476d1d4f5aa5c635f128950	
Vendor: GE					
Product: digital_industrial_gateway_server					
Affected Version(s): * Up to (including) 7.612					
Integer Overflow or Wraparound	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0754**	N/A	A-GE-DIGI-160323/222
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0755**	N/A	A-GE-DIGI-160323/223
Vendor: Genetechsolutions					
Product: pie_register					
Affected Version(s): * Up to (excluding) 3.8.2.3					
URL Redirection to	27-Feb-2023	5.4	The Registration Forms WordPress plugin before 3.8.2.3	N/A	A-GEN-PIE_-160323/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			does not properly validate the redirection URL when logging in and login out, leading to an Open Redirect vulnerability **CVE ID : CVE-2023-0552**		
Vendor: Gentoo					
Product: soko					
Affected Version(s): * Up to (excluding) 1.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	9.1	Gentoo soko is the code that powers packages.gentoo.org. Versions prior to 1.0.1 are vulnerable to SQL Injection, leading to a Denial of Service. If the user selects (in user preferences) the "Recently Visited Packages" view for the index page, the value of the `search_history` cookie is used as a base64 encoded comma separated list of atoms. These are string loaded directly into the SQL query with `atom = '%s'` format string. As a result, any user can modify the browser's cookie value and inject most SQL queries. A proof of concept malformed cookie was	https://gitweb.gentoo.org/sites/soko.git/commit/?id=5ae9ca83b735804f2bd405592983a73d7fcc42f4, https://github.com/gentoo/soko/security/advisories/GHSA-gp8g-jfq9-5q2g	A-GEN-SOKO-160323/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generated that wiped the database or changed it's content. On the database, only public data is stored, so there is no confidentiality issues to site users. If it is known that the database was modified, a full restoration of data is possible by performing a full database wipe and performing full update of all components. This issue is patched with commit id 5ae9ca83b73. Version 1.0.1 contains the patch. If users are unable to upgrade immediately, the following workarounds may be applied: (1.) Use a proxy to always drop the `search_history` cookie until upgraded. The impact on user experience is low. (2.) Sanitize to the value of `search_history` cookie after base64 decoding it. **CVE ID : CVE-2023-26033**		
Vendor: geotools					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: geotools					
Affected Version(s): * Up to (excluding) 24.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC Filters with JDBCDataStore implementations. Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue. Users unable to upgrade may disable `encode functions` for PostGIS DataStores or enable `prepared statements` for JDBCDataStores as a partial mitigation. **CVE ID : CVE-2023-25158**	https://github.com/geotools/geotools/commit/64fb4c47f43ca818c2fe96a94651bff1b3b3ed2b, https://github.com/geotools/geotools/security/advisories/GHSA-99c3-qc2q-p94m	A-GEO-GEOT-160323/226
Affected Version(s): From (including) 25.0 Up to (excluding) 25.7					
Improper Neutralization of Special Elements used in an	21-Feb-2023	9.8	GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC	https://github.com/geotools/geotools/commit/64fb4c47f43ca818c2fe96a94651bf	A-GEO-GEOT-160323/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC Filters with JDBCDataStore implementations. Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue. Users unable to upgrade may disable `encode functions` for PostGIS DataStores or enable `prepared statements` for JDBCDataStores as a partial mitigation. **CVE ID : CVE-2023-25158**	f1b3b3ed2b, https://github.com/geotools/geotools/security/advisories/GHSA-99c3-qc2q-p94m	
Affected Version(s): From (including) 26.0 Up to (excluding) 26.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC	https://github.com/geotools/geotools/commit/64fb4c47f43ca818c2fe96a94651bff1b3b3ed2b, https://github.com/geotools/geotools/security/advisories/GHSA-99c3-qc2q-p94m	A-GEO-GEOT-160323/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Filters with JDBCDataStore implementations. Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue. Users unable to upgrade may disable `encode functions` for PostGIS DataStores or enable `prepared statements` for JDBCDataStores as a partial mitigation. **CVE ID : CVE-2023-25158**		
Affected Version(s): From (including) 27.0 Up to (excluding) 27.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC Filters with JDBCDataStore implementations. Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue. Users unable to upgrade may	https://github.com/geotools/geotools/commit/64fb4c47f43ca818c2fe96a94651bff1b3b3ed2b, https://github.com/geotools/geotools/security/advisories/GHSA-99c3-qc2q-p94m	A-GEO-GEOT-160323/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disable `encode functions` for PostGIS DataStores or enable `prepared statements` for JDBCDataStores as a partial mitigation. **CVE ID : CVE-2023-25158**		
Affected Version(s): From (including) 28.0 Up to (excluding) 28.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoTools is an open source Java library that provides tools for geospatial data. GeoTools includes support for OGC Filter expression language parsing, encoding and execution against a range of datastore. SQL Injection Vulnerabilities have been found when executing OGC Filters with JDBCDataStore implementations. Users are advised to upgrade to either version 27.4 or to 28.2 to resolve this issue. Users unable to upgrade may disable `encode functions` for PostGIS DataStores or enable `prepared statements` for JDBCDataStores as a partial mitigation.	https://github.com/geotools/geotools/commit/64fb4c47f43ca818c2fe96a94651bff1b3b3ed2b, https://github.com/geotools/geotools/security/advisories/GHSA-99c3-qc2q-p94m	A-GEO-GEOT-160323/230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25158		
Vendor: Github					
Product: enterprise_server					
Affected Version(s): From (including) 3.7.0 Up to (excluding) 3.7.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	6.5	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed arbitrary file reading when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.6. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-22380**	https://docs.github.com/en/enterprise-server@3.7/admin/release-notes#3.7.6	A-GIT-ENTE-160323/231
Vendor: Gluster					
Product: glusterfs					
Affected Version(s): 11.0					
Out-of-bounds Read	21-Feb-2023	7.5	In Gluster GlusterFS 11.0, there is an xlators/mount/fuse/src/fuse-bridge.c	https://github.com/gluster/glusterfs/issues/3954	A-GLU-GLUS-160323/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			notify stack-based buffer over-read. **CVE ID : CVE-2023-26253**		
Vendor: Gnome					
Product: epiphany					
Affected Version(s): * Up to (excluding) 43.1					
Exposure of Resource to Wrong Sphere	20-Feb-2023	7.5	In Epiphany (aka GNOME Web) through 43.0, untrusted web content can trick users into exfiltrating passwords, because autofill occurs in sandboxed contexts. **CVE ID : CVE-2023-26081**	https://gitlab.gnome.org/GNOME/epiphany/-/merge_requests/1275	A-GNO-EPIP-160323/233
Vendor: gnpublisher					
Product: gn_publisher					
Affected Version(s): * Up to (including) 1.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Feb-2023	6.1	The GN Publisher plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in versions up to, and including, 1.5.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a	N/A	A-GNP-GN_P-160323/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user into performing an action such as clicking on a link. **CVE ID : CVE-2023-1080**		
Vendor: GNU					
Product: libmicrohttpd					
Affected Version(s): * Up to (excluding) 0.9.76					
Out-of-bounds Read	28-Feb-2023	7.5	GNU libmicrohttpd before 0.9.76 allows remote DoS (Denial of Service) due to improper parsing of a multipart/form-data boundary in the postprocessor.c MHD_create_post_processor() method. This allows an attacker to remotely send a malicious HTTP POST packet that includes one or more '\0' bytes in a multipart/form-data boundary field, which - assuming a specific heap layout - will result in an out-of-bounds read and a crash in the find_boundary() function. **CVE ID : CVE-2023-27371**	https://git.gnunet.org/libmicrohttpd.git/commit/?id=6d6846e20bfdf4b3eb1b592c97520a532f724238	A-GNU-LIBM-160323/235
Vendor: go-redrock					
Product: tutortrac					
Affected Version(s): * Up to (excluding) 4.2.170210					
Improper Neutralization of	21-Feb-2023	5.4	Multiple stored cross-site scripting (XSS) vulnerabilities	N/A	A-GO--TUTO-160323/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			in Redrock Software TutorTrac before v4.2.170210 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the reason and location fields of the visits listing page. **CVE ID : CVE-2023-24081**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 110.0.5481.177					
Use After Free	22-Feb-2023	8.8	Use after free in Web Payments API in Google Chrome on Android prior to 110.0.5481.177 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0927**	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	A-GOO-CHRO-160323/237
Use After Free	22-Feb-2023	8.8	Use after free in SwiftShader in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	A-GOO-CHRO-160323/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: High) **CVE ID : CVE-2023-0928**		
Use After Free	22-Feb-2023	8.8	Use after free in Vulkan in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0929**	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	A-GOO-CHRO-160323/239
Out-of-bounds Write	22-Feb-2023	8.8	Heap buffer overflow in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0930**	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	A-GOO-CHRO-160323/240
Use After Free	22-Feb-2023	8.8	Use after free in Video in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	A-GOO-CHRO-160323/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0931		
Use After Free	22-Feb-2023	8.8	Use after free in WebRTC in Google Chrome on Windows prior to 110.0.5481.177 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0932**	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	A-GOO-CHRO-160323/242
Integer Overflow or Wraparound	22-Feb-2023	8.8	Integer overflow in PDF in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium) **CVE ID : CVE-2023-0933**	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	A-GOO-CHRO-160323/243
Use After Free	22-Feb-2023	8.8	Use after free in Prompts in Google Chrome prior to 110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	A-GOO-CHRO-160323/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: Critical) **CVE ID : CVE-2023-0941**		
Vendor: gpac					
Product: gpac					
Affected Version(s): * Up to (including) 2.2.0					
Heap-based Buffer Overflow	16-Feb-2023	7.8	Heap-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.3.0-DEV. **CVE ID : CVE-2023-0866**	https://huntr.dev/bounties/7d3c5792-d20b-4cb6-9c6d-bb14f3430d7f, https://github.com/gpac/gpac/commit/b964fe4226f1424cf676d5822ef898b6b01f5937	A-GPA-GPAC-160323/245
Vendor: gradio_project					
Product: gradio					
Affected Version(s): * Up to (excluding) 3.13.1					
Use of Hard-coded Credentials	23-Feb-2023	9.8	Gradio is an open-source Python library to build machine learning and data science demos and web applications. Versions prior to 3.13.1 contain Use of Hard-coded Credentials. When using Gradio's share links (i.e. creating a Gradio app and then setting `share=True`), a private SSH key is	https://github.com/gradio-app/gradio/security/advisories/GHSA-3x5j-9vwr-8rr5	A-GRA-GRAD-160323/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to any user that connects to the Gradio machine, which means that a user could access other users' shared Gradio demos. From there, other exploits are possible depending on the level of access/exposure the Gradio app provides. This issue is patched in version 3.13.1, however, users are recommended to update to 3.19.1 or later where the FRP solution has been properly tested. **CVE ID : CVE-2023-25823**		
Vendor: greenshiftwp					
Product: greenshift_-_animation_and_page_builder_blocks					
Affected Version(s): * Up to (excluding) 5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Greenshift WordPress plugin before 5.0 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	N/A	A-GRE-GREE-160323/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0378		
Vendor: gsplugins					
Product: gs_books_showcase					
Affected Version(s): * Up to (excluding) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The GS Books Showcase WordPress plugin before 1.3.1 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-2023-0541**	N/A	A-GSP-GS_B-160323/248
Product: gs_filterable_portfolio					
Affected Version(s): * Up to (excluding) 1.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The GS Filterable Portfolio WordPress plugin before 1.6.1 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	N/A	A-GSP-GS_F-160323/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0540**		
Product: gs_insever_portfolio					
Affected Version(s): * Up to (excluding) 1.4.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	The GS Insever Portfolio WordPress plugin before 1.4.5 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-2023-0539**	N/A	A-GSP-GS_I-160323/250
Product: gs_portfolio_for_envato					
Affected Version(s): * Up to (excluding) 1.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The GS Portfolio for Envato WordPress plugin before 1.4.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embedded, which could allow users with the contributor role and above to perform Stored	N/A	A-GSP-GS_P-160323/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Scripting attacks **CVE ID : CVE-2023-0559**		
Product: gs_products_slider					
Affected Version(s): * Up to (excluding) 1.5.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The GS Products Slider for WooCommerce WordPress plugin before 1.5.9 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-2023-0492**	N/A	A-GSP-GS_P-160323/252
Vendor: hashicorp					
Product: go-getter					
Affected Version(s): * Up to (including) 1.6.2					
N/A	16-Feb-2023	6.5	HashiCorp go-getter up to 1.6.2 and 2.1.1 is vulnerable to decompression bombs. Fixed in 1.7.0 and 2.2.0. **CVE ID : CVE-2023-0475**	https://discuss.hashicorp.com/t/hcsec-2023-4-go-getter-vulnerable-to-denial-of-service-via-malicious-compressed-archive/50125	A-HAS-GO-G-160323/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.1.1					
N/A	16-Feb-2023	6.5	HashiCorp go-getter up to 1.6.2 and 2.1.1 is vulnerable to decompression bombs. Fixed in 1.7.0 and 2.2.0. **CVE ID : CVE-2023-0475**	https://discuss.hashicorp.com/t/hcsec-2023-4-go-getter-vulnerable-to-denial-of-service-via-malicious-compressed-archive/50125	A-HAS-GO-G-160323/254
Product: nomad					
Affected Version(s): * Up to (excluding) 1.2.15					
N/A	16-Feb-2023	6.5	HashiCorp Nomad and Nomad Enterprise 1.2.15 up to 1.3.8, and 1.4.3 jobs using a maliciously compressed artifact stanza source can cause excessive disk usage. Fixed in 1.2.16, 1.3.9, and 1.4.4. **CVE ID : CVE-2023-0821**	https://discuss.hashicorp.com/t/hcsec-2023-05-nomad-client-vulnerable-to-decompression-bombs-in-artifact-block/50292	A-HAS-NOMA-160323/255
Affected Version(s): From (including) 1.3.0 Up to (excluding) 1.3.9					
N/A	16-Feb-2023	6.5	HashiCorp Nomad and Nomad Enterprise 1.2.15 up to 1.3.8, and 1.4.3 jobs using a maliciously compressed artifact stanza source can cause excessive disk usage. Fixed in	https://discuss.hashicorp.com/t/hcsec-2023-05-nomad-client-vulnerable-to-decompression-bombs-in-artifact-block/50292	A-HAS-NOMA-160323/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.2.16, 1.3.9, and 1.4.4. **CVE ID : CVE-2023-0821**		
Affected Version(s): From (including) 1.4.0 Up to (excluding) 1.4.4					
N/A	16-Feb-2023	6.5	HashiCorp Nomad and Nomad Enterprise 1.2.15 up to 1.3.8, and 1.4.3 jobs using a maliciously compressed artifact stanza source can cause excessive disk usage. Fixed in 1.2.16, 1.3.9, and 1.4.4. **CVE ID : CVE-2023-0821**	https://discuss.hashicorp.com/t/hcsec-2023-05-nomad-client-vulnerable-to-decompression-bombs-in-artifact-block/50292	A-HAS-NOMA-160323/257
Vendor: hasthemes					
Product: extensions_for_cf7					
Affected Version(s): * Up to (excluding) 2.0.9					
Cross-Site Request Forgery (CSRF)	17-Feb-2023	4.3	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes Extensions For CF7 plugin <= 2.0.8 versions leads to arbitrary plugin activation. **CVE ID : CVE-2023-23899**	N/A	A-HAS-EXTE-160323/258
Product: shoplentor					
Affected Version(s): * Up to (excluding) 2.5.4					
Deserialization of Untrusted Data	21-Feb-2023	9.8	The ShopLentor WordPress plugin before 2.5.4 unserializes user input from cookies in	https://plugins.trac.wordpress.org/changeset/2852711/woolentor-	A-HAS-SHOP-160323/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			order to track viewed products and user data, which could lead to PHP Object Injection. **CVE ID : CVE-2023-0232**	addons/trunk/includes/helper-function.php	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The ShopLentor WordPress plugin before 2.5.4 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0231**	N/A	A-HAS-SHOP-160323/260
Vendor: Haxx					
Product: curl					
Affected Version(s): From (including) 7.57.0 Up to (excluding) 7.88.0					
Allocation of Resources Without Limits or Throttling	23-Feb-2023	7.5	An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning that a server response can be compressed multiple times and potentially with differentalgorithms.	https://security.netapp.com/advisory/ntap-20230309-0006/	A-HAX-CURL-160323/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors. **CVE ID : CVE-2023-23916**		
Affected Version(s): From (including) 7.77.0 Up to (excluding) 7.88.0					
Cleartext Transmission of Sensitive Information	23-Feb-2023	9.1	A cleartext transmission of sensitive information vulnerability exists in curl <v7.88.0 that could cause HSTS functionality fail when multiple URLs are requested serially. Using its HSTS support, curl can be instructed to use HTTPS instead of usingan insecure clear-text HTTP step	https://security.netapp.com/advisory/ntap-20230309-0006/	A-HAX-CURL-160323/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			even when HTTP is provided in the URL. ThisHSTS mechanism would however surprisingly be ignored by subsequent transferswhen done on the same command line because the state would not be properlycarried on. **CVE ID : CVE-2023-23914**		
Cleartext Transmission of Sensitive Information	23-Feb-2023	6.5	A cleartext transmission of sensitive information vulnerability exists in curl <v7.88.0 that could cause HSTS functionality to behave incorrectly when multiple URLs are requested in parallel. Using its HSTS support, curl can be instructed to use HTTPS instead of using an insecure clear-text HTTP step even when HTTP is provided in the URL. This HSTS mechanism would however surprisingly fail when multiple transfers are done in parallel as the HSTS cache file gets overwritten by the	https://security.netapp.com/advisory/ntap-20230309-0006/	A-HAX-CURL-160323/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			most recentlycompleted transfer. A later HTTP-only transfer to the earlier host name would then *not* get upgraded properly to HSTS. **CVE ID : CVE-2023-23915**		
Vendor: hour_of_code_python_2015_project					
Product: hour_of_code_python_2015					
Affected Version(s): 2015-12-11					
N/A	22-Feb-2023	9.8	hour_of_code_python_2015 commit 520929797b9ca43bb818b2e8f963fb2025459fa3 was discovered to contain a code execution backdoor via the request package (requirements.txt). This vulnerability allows attackers to access sensitive user information and execute arbitrary code. **CVE ID : CVE-2023-24107**	N/A	A-HOU-HOUR-160323/264
Vendor: IBM					
Product: aspera_faspex					
Affected Version(s): * Up to (including) 4.4.1					
Improper Neutralization of Input During Web Page	17-Feb-2023	5.4	IBM Aspera Faspex 4.4.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary	https://www.ibm.com/support/pages/node/6952319, https://exchange.xforce.ibm	A-IBM-ASPE-160323/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244117. **CVE ID : CVE-2023-22868**	cloud.com/vulnerabilities/244117	
Affected Version(s): 4.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	5.4	IBM Aspera Faspex 4.4.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244117. **CVE ID : CVE-2023-22868**	https://www.ibm.com/support/pages/node/6952319, https://exchange.xforce.ibmcloud.com/vulnerabilities/244117	A-IBM-ASPE-160323/266
Product: cloud_pak_for_business_automation					
Affected Version(s): 18.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100, https://www.ibm.com/support/pages/node/6958062	A-IBM-CLOU-160323/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**		
Affected Version(s): 18.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100, https://www.ibm.com/support/pages/node/6958062	A-IBM-CLOU-160323/268
Affected Version(s): 19.0.1					
Improper Neutralization of Input During	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3,	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100,	A-IBM-CLOU-160323/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**	https://www.ibm.com/support/pages/node/6958062	
Affected Version(s): 19.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100, https://www.ibm.com/support/pages/node/6958062	A-IBM-CLOU-160323/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 20.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100, https://www.ibm.com/support/pages/node/6958062	A-IBM-CLOU-160323/271
Affected Version(s): 20.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100, https://www.ibm.com/support/pages/node/6958062	A-IBM-CLOU-160323/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**		
Affected Version(s): 21.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100, https://www.ibm.com/support/pages/node/6958062	A-IBM-CLOU-160323/273
Affected Version(s): 21.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100, https://www.ibm.com/support/pages/node/6958062	A-IBM-CLOU-160323/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**		
Affected Version(s): 21.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100, https://www.ibm.com/support/pages/node/6958062	A-IBM-CLOU-160323/275
Affected Version(s): 22.0.1					
Improper Neutralization of Input During Web Page	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3,	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100, https://www.i	A-IBM-CLOU-160323/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**	bm.com/support/pages/node/6958062	
Affected Version(s): 22.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244100. **CVE ID : CVE-2023-22860**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244100, https://www.ibm.com/support/pages/node/6958062	A-IBM-CLOU-160323/277
Product: infosphere_information_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 11.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Feb-2023	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 246333 **CVE ID : CVE-2023-24960**	https://www.ibm.com/support/pages/node/6953521, https://exchange.xforce.ibmcloud.com/vulnerabilities/246333	A-IBM-INFO-160323/278
Cleartext Storage of Sensitive Information	17-Feb-2023	5.5	IBM InfoSphere Information Server 11.7 could allow a local user to obtain sensitive information from a log files. IBM X-Force ID: 246463. **CVE ID : CVE-2023-24964**	https://exchange.xforce.ibmcloud.com/vulnerabilities/246463, https://www.ibm.com/support/pages/node/6953519	A-IBM-INFO-160323/279
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247646.	https://exchange.xforce.ibmcloud.com/vulnerabilities/247646, https://www.ibm.com/support/pages/node/6956598	A-IBM-INFO-160323/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25928		
Vendor: jd-gui_project					
Product: jd-gui					
Affected Version(s): 1.6.6					
Deserialization of Untrusted Data	21-Feb-2023	9.8	JD-GUI 1.6.6 allows deserialization via UIMainWindowPreferencesProvider.singleInstance. **CVE ID : CVE-2023-26234**	N/A	A-JD--JD-G-160323/281
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	JD-GUI 1.6.6 allows XSS via util/net/InterProcessCommunicationUtil.java. **CVE ID : CVE-2023-26235**	https://github.com/java-decompiler/jd-gui/pull/418	A-JD--JD-G-160323/282
Vendor: Joomla					
Product: joomla\!					
Affected Version(s): From (including) 4.0.0 Up to (including) 4.2.7					
N/A	16-Feb-2023	5.3	An issue was discovered in Joomla! 4.0.0 through 4.2.7. An improper access check allows unauthorized access to webservice endpoints. **CVE ID : CVE-2023-23752**	https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html	A-JOO-JOOM-160323/283
Vendor: joomunited					
Product: wp_meta_seo					
Affected Version(s): * Up to (including) 4.5.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized options update due to a missing capability check on the wpmsGGSaveInformation function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to update google analytics options maintained by the plugin. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role. **CVE ID : CVE-2023-1022**	https://plugins.trac.wordpress.org/changeset/2870465/wp-meta-seo/trunk?contextall=1&old=2869205&old_path=%2Fwp-meta-seo%2Ftrunk#file2, https://www.wordfence.com/threat-intel/vulnerabilities/id/702f9d3b-5d33-4215-ac76-9aae3162d775	A-JOO-WP_M-160323/284
Missing Authorization	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the saveSitemapSettings	https://plugins.trac.wordpress.org/changeset/2870465/wp-meta-seo/trunk?contextall=1&old=2869205&old_path=%2Fwp-meta-	A-JOO-WP_M-160323/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to change sitemap-related settings of the plugin. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role. **CVE ID : CVE-2023-1023**	seo%2Ftrunk#file2, https://www.wordfence.com/threat-intel/vulnerabilities/id/9d1e498a-ddcb-4c67-bf0d-bb45b6fe0e9d	
Missing Authorization	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized sitemap generation due to a missing capability check on the regenerateSitemaps function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to generate sitemaps. This vulnerability occurred as a result	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2870465%40wp-meta-seo&new=2870465%40wp-meta-seo&sfp_email=&sfph_mail=	A-JOO-WP_M-160323/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role. **CVE ID : CVE-2023-1024**		
Missing Authorization	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the listPostsCategory function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to get post listings by category as long as those posts are published. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role. **CVE ID : CVE-2023-1026**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2870465%40wp-meta-seo&new=2870465%40wp-meta-seo&sfp_email=&sfph_mail=	A-JOO-WP_M-160323/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to unauthorized sitemap generation due to a missing capability check on the checkAllCategoryInSitemap function in versions up to, and including, 4.5.3. This makes it possible for authenticated attackers with subscriber-level access to obtain post categories. This vulnerability occurred as a result of the plugin relying on nonce checks as a means of access control, and that nonce being accessible to all authenticated users regardless of role. **CVE ID : CVE-2023-1027**	https://plugins.trac.wordpress.org/changeset/2870465/wp-meta-seo/trunk?contextall=1&old=2869205&old_path=%2Fwp-meta-seo%2Ftrunk#file2	A-JOO-WP_M-160323/288
Cross-Site Request Forgery (CSRF)	28-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.5.3. This is due to missing or incorrect nonce validation on the setIgnore function. This makes it	https://plugins.trac.wordpress.org/changeset/2870465/wp-meta-seo/trunk?contextall=1&old=2869205&old_path=%2Fwp-meta-seo%2Ftrunk#file2,	A-JOO-WP_M-160323/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for unauthenticated attackers to update plugin options via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1028**	https://plugins.trac.wordpress.org/changeset/2870465/wp-meta-seo/tags/4.5.4/inc/class.metaseo-admin.php	
Cross-Site Request Forgery (CSRF)	24-Feb-2023	4.3	The WP Meta SEO plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.5.3. This is due to missing or incorrect nonce validation on the regenerateSitemaps function. This makes it possible for unauthenticated attackers to regenerate Sitemaps via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1029**	N/A	A-JOO-WP_M-160323/290
Vendor: judging_management_system_project					
Product: judging_management_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	23-Feb-2023	8.1	Judging Management System 1.0 was discovered to contain an arbitrary file upload vulnerability via the component edit_organizer.php. **CVE ID : CVE-2023-24317**	N/A	A-JUD-JUDG-160323/291
Vendor: kainelabs					
Product: youzify					
Affected Version(s): * Up to (excluding) 1.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Youzify WordPress plugin before 1.2.2 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-2023-0059**	N/A	A-KAI-YOUZ-160323/292
Vendor: kavitareader					
Product: kavita					
Affected Version(s): * Up to (excluding) 0.7.0					
Missing Authentication for Critical Function	19-Feb-2023	3.5	Missing Authentication for Critical Function in GitHub repository kareadita/kavita prior to 0.7.0.	https://github.com/kareadita/kavita/commit/6648b79e1b2f92449d5816d0722b7a3d72f259d5,	A-KAV-KAVI-160323/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0919	https://huntr.dev/bounties/3c514923-473f-4c50-ae0d-d002a41fe70f	
Vendor: Kibokolabs					
Product: arigato_autoresponder_and_newsletter					
Affected Version(s): * Up to (excluding) 2.1.7.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	4.8	The Arigato Autoresponder and Newsletter WordPress plugin before 2.1.7.2 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2023-0543**	N/A	A-KIB-ARIG-160323/294
Product: namaste\!_lms					
Affected Version(s): * Up to (excluding) 2.5.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	4.8	The Namaste! LMS WordPress plugin before 2.5.9.4 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html	N/A	A-KIB-NAMA-160323/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-0548**		
Product: watu_quiz					
Affected Version(s): * Up to (excluding) 3.3.8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	The Watu Quiz WordPress plugin before 3.3.8.2 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 against high privilege users such as admin. **CVE ID : CVE-2023-0428**	N/A	A-KIB-WATU-160323/296
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	4.8	The Watu Quiz WordPress plugin before 3.3.8.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	N/A	A-KIB-WATU-160323/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0429		
Vendor: krontech					
Product: single_connect					
Affected Version(s): * Up to (excluding) 2.16.1					
Authorization Bypass Through User-Controlled Key	17-Feb-2023	8.8	Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Kron Tech Single Connect on Windows allows Privilege Abuse. This issue affects Single Connect: 2.16. **CVE ID : CVE-2023-0882**	https://docs.krontech.com/singleconnect-2-16/update-patch-rdp-proxy-idor-vulnerability	A-KRO-SING-160323/298
Vendor: laravel-admin					
Product: laravel-admin					
Affected Version(s): 1.8.19					
Unrestricted Upload of File with Dangerous Type	27-Feb-2023	7.2	An arbitrary file upload vulnerability in laravel-admin v1.8.19 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2023-24249**	N/A	A-LAR-LARA-160323/299
Vendor: Libreswan					
Product: libreswan					
Affected Version(s): 4.9					
Uncontrolled Resource Consumption	21-Feb-2023	6.5	Libreswan 4.9 allows remote attackers to cause a denial of service (assert failure and daemon restart) via crafted	https://github.com/libreswan/libreswan/issues/954	A-LIB-LIBR-160323/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TS payload with an incorrect selector length. **CVE ID : CVE-2023-23009**		
Vendor: Linuxfoundation					
Product: argo-cd					
Affected Version(s): From (including) 2.3.0 Up to (excluding) 2.3.17					
Incorrect Authorization	16-Feb-2023	8.5	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All Argo CD versions starting with 2.3.0-rc1 and prior to 2.3.17, 2.4.23 2.5.11, and 2.6.2 are vulnerable to an improper authorization bug which allows users who have the ability to update at least one cluster secret to update any cluster secret. The attacker could use this access to escalate privileges (potentially controlling Kubernetes resources) or to break Argo CD functionality (by preventing connections to external clusters). A patch for this vulnerability has been released in Argo CD versions 2.6.2, 2.5.11, 2.4.23,	https://github.com/argoproj/argo-cd/commit/fbb0b99b1ac3361b253052bd30259fa43a520945, https://github.com/argoproj/argo-cd/security/advisories/GHSA-3jfq-742w-xg8j	A-LIN-ARGO-160323/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 2.3.17. Two workarounds are available. Either modify the RBAC configuration to completely revoke all `clusters, update` access, or use the `destinations` and `clusterResourceWhitelist` fields to apply similar restrictions as the `namespaces` and `clusterResources` fields. **CVE ID : CVE-2023-23947**		
Affected Version(s): From (including) 2.4.0 Up to (excluding) 2.4.23					
Incorrect Authorization	16-Feb-2023	8.5	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All Argo CD versions starting with 2.3.0-rc1 and prior to 2.3.17, 2.4.23 2.5.11, and 2.6.2 are vulnerable to an improper authorization bug which allows users who have the ability to update at least one cluster secret to update any cluster secret. The attacker could use this access to escalate privileges (potentially controlling Kubernetes resources) or to	https://github.com/argoproj/argo-cd/commit/fbb0b99b1ac3361b253052bd30259fa43a520945, https://github.com/argoproj/argo-cd/security/advisories/GHSA-3jfq-742w-xg8j	A-LIN-ARGO-160323/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			break Argo CD functionality (by preventing connections to external clusters). A patch for this vulnerability has been released in Argo CD versions 2.6.2, 2.5.11, 2.4.23, and 2.3.17. Two workarounds are available. Either modify the RBAC configuration to completely revoke all `clusters, update` access, or use the `destinations` and `clusterResourceWhitelist` fields to apply similar restrictions as the `namespaces` and `clusterResources` fields. **CVE ID : CVE-2023-23947**		
Affected Version(s): From (including) 2.5.0 Up to (excluding) 2.5.11					
Incorrect Authorization	16-Feb-2023	8.5	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All Argo CD versions starting with 2.3.0-rc1 and prior to 2.3.17, 2.4.23 2.5.11, and 2.6.2 are vulnerable to an improper authorization bug which allows users who have the ability	https://github.com/argoproj/argo-cd/commit/fbb0b99b1ac3361b253052bd30259fa43a520945, https://github.com/argoproj/argo-cd/security/advisories/GHS	A-LIN-ARGO-160323/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to update at least one cluster secret to update any cluster secret. The attacker could use this access to escalate privileges (potentially controlling Kubernetes resources) or to break Argo CD functionality (by preventing connections to external clusters). A patch for this vulnerability has been released in Argo CD versions 2.6.2, 2.5.11, 2.4.23, and 2.3.17. Two workarounds are available. Either modify the RBAC configuration to completely revoke all `clusters, update` access, or use the `destinations` and `clusterResourceWhitelist` fields to apply similar restrictions as the `namespaces` and `clusterResources` fields. **CVE ID : CVE-2023-23947**	A-3jfq-742w-xg8j	
Affected Version(s): From (including) 2.6.0 Up to (excluding) 2.6.2					
Incorrect Authorization	16-Feb-2023	8.5	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes.	https://github.com/argoproj/argo-cd/commit/fb	A-LIN-ARGO-160323/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			All Argo CD versions starting with 2.3.0-rc1 and prior to 2.3.17, 2.4.23 2.5.11, and 2.6.2 are vulnerable to an improper authorization bug which allows users who have the ability to update at least one cluster secret to update any cluster secret. The attacker could use this access to escalate privileges (potentially controlling Kubernetes resources) or to break Argo CD functionality (by preventing connections to external clusters). A patch for this vulnerability has been released in Argo CD versions 2.6.2, 2.5.11, 2.4.23, and 2.3.17. Two workarounds are available. Either modify the RBAC configuration to completely revoke all `clusters, update` access, or use the `destinations` and `clusterResourceWhitelist` fields to apply similar restrictions as the `namespaces` and	b0b99b1ac3361b253052bd30259fa43a520945, https://github.com/argoproj/argo-cd/security/advisories/GHSA-3jfq-742w-xg8j	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`clusterResources` fields. **CVE ID : CVE-2023-23947**		
Product: containerd					
Affected Version(s): * Up to (excluding) 1.5.18					
Incorrect Authorization	16-Feb-2023	7.8	containerd is an open source container runtime. A bug was found in containerd prior to versions 1.6.18 and 1.5.18 where supplementary groups are not set up properly inside a container. If an attacker has direct access to a container and manipulates their supplementary group access, they may be able to use supplementary group access to bypass primary group restrictions in some cases, potentially gaining access to sensitive information or gaining the ability to execute code in that container. Downstream applications that use the containerd client library may be affected as well. This bug has been fixed in containerd v1.6.18 and v.1.5.18. Users should update to	https://github.com/containerd/containerd/commit/133f6bb6cd827ce35a5fb279c1ead12b9d21460a, https://github.com/containerd/containerd/security/advisories/GHSA-hmfx-3pcx-653p	A-LIN-CONT-160323/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these versions and recreate containers to resolve this issue. Users who rely on a downstream application that uses containerd's client library should check that application for a separate advisory and instructions. As a workaround, ensure that the `"USER $USERNAME"` Dockerfile instruction is not used. Instead, set the container entrypoint to a value similar to `ENTRYPOINT ["su", "-", "user"]` to allow `su` to properly set up supplementary groups. **CVE ID : CVE-2023-25173**		
Allocation of Resources Without Limits or Throttling	16-Feb-2023	5.5	containerd is an open source container runtime. Before versions 1.6.18 and 1.5.18, when importing an OCI image, there was no limit on the number of bytes read for certain files. A maliciously crafted image with a large file where a limit was not applied could cause a denial of service. This bug has	https://github.com/containerd/containerd/commit/0c314901076a74a7b797a545d2f462285fdbb8c4, https://github.com/containerd/containerd/security/advisories/GHSA-259w-8hf6-59c2	A-LIN-CONT-160323/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been fixed in containerd 1.6.18 and 1.5.18. Users should update to these versions to resolve the issue. As a workaround, ensure that only trusted images are used and that only trusted users have permissions to import images. **CVE ID : CVE-2023-25153**		
Affected Version(s): From (including) 1.6.0 Up to (excluding) 1.6.18					
Incorrect Authorization	16-Feb-2023	7.8	containerd is an open source container runtime. A bug was found in containerd prior to versions 1.6.18 and 1.5.18 where supplementary groups are not set up properly inside a container. If an attacker has direct access to a container and manipulates their supplementary group access, they may be able to use supplementary group access to bypass primary group restrictions in some cases, potentially gaining access to sensitive information or gaining the ability to execute code in that	https://github.com/containerd/containerd/commit/133f6bb6cd827ce35a5fb279c1ead12b9d21460a, https://github.com/containerd/containerd/security/advisories/GHSA-hmfx-3pcx-653p	A-LIN-CONT-160323/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			container. Downstream applications that use the containerd client library may be affected as well. This bug has been fixed in containerd v1.6.18 and v.1.5.18. Users should update to these versions and recreate containers to resolve this issue. Users who rely on a downstream application that uses containerd's client library should check that application for a separate advisory and instructions. As a workaround, ensure that the `"USER $USERNAME"` Dockerfile instruction is not used. Instead, set the container entrypoint to a value similar to `ENTRYPOINT ["su", "-", "user"]` to allow `su` to properly set up supplementary groups. **CVE ID : CVE-2023-25173**		
Allocation of Resources Without Limits or Throttling	16-Feb-2023	5.5	containerd is an open source container runtime. Before versions 1.6.18 and 1.5.18, when importing an	https://github.com/containerd/containerd/commit/0c314901076a74a7b797a545d	A-LIN-CONT-160323/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OCI image, there was no limit on the number of bytes read for certain files. A maliciously crafted image with a large file where a limit was not applied could cause a denial of service. This bug has been fixed in containerd 1.6.18 and 1.5.18. Users should update to these versions to resolve the issue. As a workaround, ensure that only trusted images are used and that only trusted users have permissions to import images. **CVE ID : CVE-2023-25153**	2f462285fdbb8c4, https://github.com/containerd/containerd/security/advisories/GHSA-259w-8hf6-59c2	
Vendor: lite-web-server_project					
Product: lite-web-server					
Affected Version(s): -					
Uncontrolled Resource Consumption	25-Feb-2023	7.5	All versions of the package lite-web-server are vulnerable to Denial of Service (DoS) when an attacker sends an HTTP request and includes control characters that the decodeURI() function is unable to parse. **CVE ID : CVE-2023-26104**	N/A	A-LIT-LITE-160323/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: loan_comparison_project					
Product: loan_comparison					
Affected Version(s): * Up to (excluding) 1.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	The Loan Comparison WordPress plugin before 1.5.3 does not validate and escape some of its query parameters before outputting them back in a page/post via an embedded shortcode, which could allow an attacker to inject javascript into into the site via a crafted URL. **CVE ID : CVE-2023-0442**	N/A	A-LOA-LOAN-160323/310
Vendor: luckyframe					
Product: luckyframeweb					
Affected Version(s): 3.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	9.8	LuckyframeWEB v3.5 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /system/UserMapper.xml. **CVE ID : CVE-2023-24219**	https://github.com/seagull1985/LuckyFrameWeb/issues/24	A-LUC-LUCK-160323/311
Improper Neutralization of Special Elements used in an	17-Feb-2023	9.8	LuckyframeWEB v3.5 was discovered to contain a SQL injection vulnerability via the dataScope parameter	https://github.com/seagull1985/LuckyFrameWeb/issues/22	A-LUC-LUCK-160323/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			at /system/RoleMapper.xml. **CVE ID : CVE-2023-24220**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	9.8	LuckyframeWEB v3.5 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /system/DeptMapper.xml. **CVE ID : CVE-2023-24221**	https://github.com/seagull1985/LuckyFrameWeb/issues/23	A-LUC-LUCK-160323/313
Vendor: mainwp					
Product: motomo					
Affected Version(s): * Up to (excluding) 4.0.5					
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in MainWP Matomo Extension <= 4.0.4 versions. **CVE ID : CVE-2023-23659**	N/A	A-MAI-MOTO-160323/314
Vendor: Mantisbt					
Product: mantisbt					
Affected Version(s): * Up to (excluding) 2.25.6					
N/A	23-Feb-2023	4.3	Mantis Bug Tracker (MantisBT) is an open source issue tracker. In versions prior to 2.25.6, due to insufficient access-level checks, any logged-in user allowed to perform Group Actions can	https://www.mantisbt.org/bugs/view.php?id=31086	A-MAN-MANT-160323/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to the _Summary_ field of private Issues (i.e. having Private view status, or belonging to a private Project) via a crafted `bug_arr[]` parameter in *bug_actiongroup_ext.php*. This issue is fixed in version 2.25.6. There are no workarounds. **CVE ID : CVE-2023-22476**		
Vendor: markdown-electron_project					
Product: markdown-electron					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	24-Feb-2023	7.8	A vulnerability was found in JP1016 Markdown-Electron and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to code injection. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are	N/A	A-MAR-MARK-160323/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			available. VDB-221738 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1005**		
Vendor: marktext					
Product: marktext					
Affected Version(s): * Up to (including) 0.17.1					
Improper Control of Generation of Code ('Code Injection')	24-Feb-2023	7.8	A vulnerability has been found in MarkText up to 0.17.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the component WSH JScript Handler. The manipulation leads to code injection. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-221737 was assigned to this vulnerability. **CVE ID : CVE-2023-1004**	N/A	A-MAR-MARK-160323/317
Vendor: mattermost					
Product: mattermost					
Affected Version(s): * Up to (including) 7.1.4					
Missing Authorization	27-Feb-2023	6.5	A missing permissions check in the /plugins/playbooks/api/v0/runs API in	https://mattermost.com/security-updates/	A-MAT-MATT-160323/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mattermost allows an attacker to list and view playbooks belonging to a team they are not a member of. **CVE ID : CVE-2023-27263**		
Missing Authorization	27-Feb-2023	6.5	A missing permissions check in Mattermost Playbooks in Mattermost allows an attacker to modify a playbook via the /plugins/playbooks/api/v0/playbooks/[playbookID] API. **CVE ID : CVE-2023-27264**	https://mattermost.com/security-updates/	A-MAT-MATT-160323/319
Affected Version(s): 7.4.0					
Missing Authorization	27-Feb-2023	6.5	A missing permissions check in the /plugins/playbooks/api/v0/runs API in Mattermost allows an attacker to list and view playbooks belonging to a team they are not a member of. **CVE ID : CVE-2023-27263**	https://mattermost.com/security-updates/	A-MAT-MATT-160323/320
Missing Authorization	27-Feb-2023	6.5	A missing permissions check in Mattermost Playbooks in Mattermost allows an attacker to modify a playbook via the /plugins/playbooks/	https://mattermost.com/security-updates/	A-MAT-MATT-160323/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			api/v0/playbooks/[playbookID] API. **CVE ID : CVE-2023-27264**		
Affected Version(s): 7.5.0					
Missing Authorization	27-Feb-2023	6.5	A missing permissions check in the /plugins/playbooks/api/v0/runs API in Mattermost allows an attacker to list and view playbooks belonging to a team they are not a member of. **CVE ID : CVE-2023-27263**	https://mattermost.com/security-updates/	A-MAT-MATT-160323/322
Missing Authorization	27-Feb-2023	6.5	A missing permissions check in Mattermost Playbooks in Mattermost allows an attacker to modify a playbook via the /plugins/playbooks/api/v0/playbooks/[playbookID] API. **CVE ID : CVE-2023-27264**	https://mattermost.com/security-updates/	A-MAT-MATT-160323/323
Affected Version(s): 7.5.1					
Missing Authorization	27-Feb-2023	6.5	A missing permissions check in the /plugins/playbooks/api/v0/runs API in Mattermost allows an attacker to list and view playbooks belonging to a team	https://mattermost.com/security-updates/	A-MAT-MATT-160323/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they are not a member of. **CVE ID : CVE-2023-27263**		
Missing Authorization	27-Feb-2023	6.5	A missing permissions check in Mattermost Playbooks in Mattermost allows an attacker to modify a playbook via the /plugins/playbooks/api/v0/playbooks/[playbookID] API. **CVE ID : CVE-2023-27264**	https://mattermost.com/security-updates/	A-MAT-MATT-160323/325
Product: mattermost_server					
Affected Version(s): From (including) 5.12.0 Up to (excluding) 7.7.0					
Exposure of Resource to Wrong Sphere	27-Feb-2023	2.7	Mattermost fails to honor the ShowEmailAddress setting when constructing a response to the "Regenerate Invite Id" API endpoint, allowing an attacker with team admin privileges to learn the team owner's email address in the response. **CVE ID : CVE-2023-27265**	https://mattermost.com/security-updates/	A-MAT-MATT-160323/326
Exposure of Sensitive Information to an Unauthorized Actor	27-Feb-2023	2.7	Mattermost fails to honor the ShowEmailAddress setting when constructing a response to the /api/v4/users/me/t	https://mattermost.com/security-updates/	A-MAT-MATT-160323/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			eams API endpoint, allowing an attacker with team admin privileges to learn the team owner's email address in the response. **CVE ID : CVE-2023-27266**		
Vendor: media_library_assistant_project					
Product: media_library_assistant					
Affected Version(s): * Up to (excluding) 3.06					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	7.2	The Media Library Assistant WordPress plugin before 3.06 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin. **CVE ID : CVE-2023-0279**	N/A	A-MED-MEDI-160323/328
Vendor: medical_certificate_generator_app_project					
Product: medical_certificate_generator_app					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2023	5.4	A vulnerability was found in SourceCodester Medical Certificate Generator App 1.0. It has been classified as problematic. This affects an unknown part of the component New Record Handler. The manipulation of the	N/A	A-MED-MEDI-160323/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument Firstname/Middlename/Lastname/Suffix/Nationality/Doctor Fullname/Doctor Suffix with the input "><script>prompt(1)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-221739. **CVE ID : CVE-2023-1006**		
Vendor: Microweber					
Product: microweber					
Affected Version(s): * Up to (including) 1.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Feb-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.3. **CVE ID : CVE-2023-1081**	https://github.com/microweber/microweber/commit/29d418461d8407688f2720e7b4be915e03fc16c1, https://huntr.dev/bounties/cf59deed-9d43-4552-acfd-43f38f3aabba	A-MIC-MICR-160323/330
Vendor: minio					
Product: minio					
Affected Version(s): From (including) 2020-04-10t03-34-42z Up to (excluding) 2023-02-17t17-52-43z					
N/A	21-Feb-2023	8.8	Minio is a Multi-Cloud Object Storage framework. Affected	https://github.com/minio/minio/securit	A-MIN-MINI-160323/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions do not correctly honor a `Deny` policy on ByPassGoverance. Ideally, minio should return "Access Denied" to all users attempting to DELETE a versionId with the special header `X-Amz-Bypass-Governance-Retention: true`. However, this was not honored instead the request will be honored and an object under governance would be incorrectly deleted. All users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25812**	y/advisories/GHSA-c8fc-mjj8-fc63, https://github.com/minio/minio/commit/a7188bc9d0f0a5ae05aaf1b8126bcd3cb3fdc485, https://github.com/minio/minio/pull/16635	
Vendor: misskey					
Product: misskey					
Affected Version(s): * Up to (excluding) 13.3.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Feb-2023	9.8	Misskey is an open source, decentralized social media platform. In versions prior to 13.3.3 SQL injection is possible due to insufficient parameter validation in the note search API by tag (notes/search-by-tag). This has been	https://github.com/misskey-dev/misskey/security/advisories/GHSA-cgwp-vmr4-wx4q, https://github.com/misskey-dev/misskey/	A-MIS-MISS-160323/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in version 13.3.3. Users are advised to upgrade. Users unable to upgrade should block access to the `api/notes/search-by-tag` endpoint. **CVE ID : CVE-2023-24812**	commit/ee74df68233adcd5b167258c621565f97c3b2306	
Affected Version(s): * Up to (excluding) 13.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	6.1	Misskey is an open source, decentralized social media platform. Due to insufficient validation of the redirect URL during `miauth` authentication in Misskey, arbitrary JavaScript can be executed when a user allows the link. All versions below 13.3.1 (including 12.x) are affected. This has been fixed in version 13.3.1. Users are advised to upgrade. Users unable to upgrade should not allow authentication of untrusted apps. **CVE ID : CVE-2023-24810**	https://github.com/misskey-dev/misskey/security/advisories/GHSA-cc6r-chgr-8r5m	A-MIS-MISS-160323/333
Affected Version(s): * Up to (excluding) 13.3.2					
Improper Neutralization of Input	22-Feb-2023	6.1	Misskey is an open source, decentralized social media platform. In versions	https://github.com/misskey-dev/misskey/	A-MIS-MISS-160323/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			prior to 13.3.2 the URL preview function is subject to a cross site scripting vulnerability due to insufficient URL validation. Arbitrary JavaScript is executed when a malicious URL is loaded in the `View in Player` or `View in Window` preview. This has been fixed in version 13.3.2. Users are advised to upgrade. Users unable to upgrade should avoid usage of the `View in Player` or `View in Window` functions. **CVE ID : CVE-2023-24811**	commit/38f9d1e76428bea47c5944c440eab25428c7d99e, https://github.com/misskey-dev/misskey/security/advisories/GHSA-vc39-c453-67g3	
Affected Version(s): * Up to (excluding) 13.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	6.1	Misskey is an open source, decentralized social media platform. In versions prior to 13.5.0 the link to the instance to the sender that appears when viewing a user or note received through ActivityPub is not properly validated, so by inserting a URL with a javascript scheme an attacker may execute JavaScript code in the context of	https://github.com/misskey-dev/misskey/security/advisories/GHSA-pfp5-r48x-fg25	A-MIS-MISS-160323/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the recipient. This issue has been fixed in version 13.5.0. Users are advised to upgrade. Users unable to upgrade should not "view on remote" for untrusted instances. **CVE ID : CVE-2023-25154**		
Vendor: modoboa					
Product: installer					
Affected Version(s): * Up to (excluding) 2.0.4					
Improper Restriction of Excessive Authentication Attempts	16-Feb-2023	7.5	Improper Restriction of Excessive Authentication Attempts in GitHub repository modoboa/modoboa-installer prior to 2.0.4. **CVE ID : CVE-2023-0860**	https://huntr.dev/bounties/64f3ab93-1357-4468-8ff4-52bbcec18cca, https://github.com/modoboa/modoboa-installer/commit/63d92b73f3da6971ae4e13d033d625773ac91085	A-MOD-INST-160323/336
Product: modoboa					
Affected Version(s): * Up to (excluding) 2.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	4.8	Cross-site Scripting (XSS) - Reflected in GitHub repository modoboa/modoboa prior to 2.0.5. **CVE ID : CVE-2023-0949**	https://github.com/modoboa/modoboa/commit/aa74e9a4a870162eea169e0a6a2eab841f8811b7, https://huntr.dev/bounties/ef87be4e-	A-MOD-MODO-160323/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				493b-4ee9-9738-44c55b8acc19	
Vendor: mod_gnutls_project					
Product: mod_gnutls					
Affected Version(s): From (including) 0.9.0 Up to (including) 1.2.0					
Loop with Unreachable Exit Condition ('Infinite Loop')	23-Feb-2023	7.5	Mod_gnutls is a TLS module for Apache HTTPD based on GnuTLS. Versions from 0.9.0 to 0.12.0 (including) did not properly fail blocking read operations on TLS connections when the transport hit timeouts. Instead it entered an endless loop retrying the read operation, consuming CPU resources. This could be exploited for denial of service attacks. If trace level logging was enabled, it would also produce an excessive amount of log output during the loop, consuming disk space. The problem has been fixed in commit d7eec4e598158ab6a98bf505354e84352f9715ec, please update to version 0.12.1. There are no workarounds, users who cannot update should apply the	https://github.com/airtower-luna/mod_gnutls/commit/d7eec4e598158ab6a98bf505354e84352f9715ec, https://github.com/airtower-luna/mod_gnutls/security/advisories/GHSA-6cfv-fvgm-7pc8, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=942737#25	A-MOD-MOD_-160323/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			errno fix detailed in the security advisory. **CVE ID : CVE-2023-25824**		
Vendor: Mono-project					
Product: mono					
Affected Version(s): 5.18.0.240\\+dfsg-3					
N/A	22-Feb-2023	8.8	The mono package before 6.8.0.105+dfsg-3.3 for Debian allows arbitrary code execution because the application/x-ms-dos-executable MIME type is associated with an un-sandboxed Mono CLR interpreter. **CVE ID : CVE-2023-26314**	N/A	A-MON-MONO-160323/339
Affected Version(s): 6.8.0.105\\+dfsg-3					
N/A	22-Feb-2023	8.8	The mono package before 6.8.0.105+dfsg-3.3 for Debian allows arbitrary code execution because the application/x-ms-dos-executable MIME type is associated with an un-sandboxed Mono CLR interpreter. **CVE ID : CVE-2023-26314**	N/A	A-MON-MONO-160323/340
Vendor: Moodle					
Product: moodle					
Affected Version(s): 4.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Feb-2023	8.2	The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality. **CVE ID : CVE-2023-23923**	https://moodle.org/mod/forum/discuss.php?d=443274#p1782023, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76862	A-MOO-MOOD-160323/341
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. **CVE ID : CVE-2023-23921**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76810, https://moodle.org/mod/forum/discuss.php?d=443272#p1782021	A-MOO-MOOD-160323/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in blog search. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. **CVE ID : CVE-2023-23922**	https://moodle.org/mod/forum/discuss.php?d=443273#p1782022, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76861	A-MOO-MOOD-160323/343
Affected Version(s): From (including) 3.11.0 Up to (excluding) 3.11.12					
N/A	17-Feb-2023	8.2	The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality. **CVE ID : CVE-2023-23923**	https://moodle.org/mod/forum/discuss.php?d=443274#p1782023, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76862	A-MOO-MOOD-160323/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. **CVE ID : CVE-2023-23921**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76810, https://moodle.org/mod/forum/discuss.php?d=443272#p1782021	A-MOO-MOOD-160323/345
Affected Version(s): From (including) 3.9.0 Up to (excluding) 3.9.19					
N/A	17-Feb-2023	8.2	The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality.	https://moodle.org/mod/forum/discuss.php?d=443274#p1782023, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76862	A-MOO-MOOD-160323/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23923		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. **CVE ID : CVE-2023-23921**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76810, https://moodle.org/mod/forum/discuss.php?d=443272#p1782021	A-MOO-MOOD-160323/347
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.6					
N/A	17-Feb-2023	8.2	The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise	https://moodle.org/mod/forum/discuss.php?d=443274#p1782023, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76862	A-MOO-MOOD-160323/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restricted functionality. **CVE ID : CVE-2023-23923**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. **CVE ID : CVE-2023-23921**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76810, https://moodle.org/mod/forum/discuss.php?d=443272#p1782021	A-MOO-MOOD-160323/349
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in blog search. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website.	https://moodle.org/mod/forum/discuss.php?d=443273#p1782022, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-76861	A-MOO-MOOD-160323/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks. **CVE ID : CVE-2023-23922**		
Vendor: moosikay_e-commerce_system_project					
Product: moosikay_e-commerce_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Feb-2023	8.8	A vulnerability was found in SourceCodester Moosikay E-Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Moosikay/order.php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221732. **CVE ID : CVE-2023-0997**	N/A	A-MOO-MOOS-160323/351
Vendor: music_gallery_site_project					
Product: music_gallery_site					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Music Gallery Site 1.0. This affects an unknown part of the file music_list.php of the component GET Request Handler. The manipulation of the argument cid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221553 was assigned to this vulnerability. **CVE ID : CVE-2023-0938**	N/A	A-MUS-MUSI-160323/352
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Feb-2023	9.8	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been classified as critical. This affects an unknown part of the file view_music_details.php of the component GET Request Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely.	N/A	A-MUS-MUSI-160323/353

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-221631. **CVE ID : CVE-2023-0961**		
Improper Access Control	22-Feb-2023	9.8	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been rated as critical. This issue affects some unknown processing of the file Users.php of the component POST Request Handler. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221633 was assigned to this vulnerability. **CVE ID : CVE-2023-0963**	N/A	A-MUS-MUSI-160323/354
Improper Neutralization of Special Elements used in an SQL Command	27-Feb-2023	9.8	A vulnerability was found in SourceCodester Music Gallery Site 1.0 and classified as critical. This issue affects some unknown processing	N/A	A-MUS-MUSI-160323/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			of the file view_category.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-221819. **CVE ID : CVE-2023-1053**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	9.8	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/?page=user/manage. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-221820. **CVE ID : CVE-2023-1054**	N/A	A-MUS-MUSI-160323/356
Improper Neutralization of Special Elements used in an SQL Command	22-Feb-2023	8.8	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been declared as critical. This vulnerability affects unknown code of the file	N/A	A-MUS-MUSI-160323/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			Master.php of the component GET Request Handler. The manipulation of the argument 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-221632. **CVE ID : CVE-2023-0962**		
Vendor: muyucms					
Product: muyucms					
Affected Version(s): 2.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Feb-2023	8.8	A vulnerability was found in MuYuCMS 2.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /editor/index.php. The manipulation of the argument file_path leads to relative path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier	N/A	A-MUY-MUYU-160323/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability is VDB-221803. **CVE ID : CVE-2023-1044**		
Server-Side Request Forgery (SSRF)	26-Feb-2023	8.8	A vulnerability classified as critical has been found in MuYuCMS 2.2. This affects an unknown part of the file /admin.php/update/getFile.html. The manipulation of the argument url leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221805 was assigned to this vulnerability. **CVE ID : CVE-2023-1046**	N/A	A-MUY-MUYU-160323/359
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Feb-2023	8.1	A vulnerability was found in MuYuCMS 2.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin.php/accessory/filesdel.html. The manipulation of the argument filedelur leads to relative path traversal. The attack may be launched remotely. The exploit	N/A	A-MUY-MUYU-160323/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221804. **CVE ID : CVE-2023-1045**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Feb-2023	6.5	A vulnerability, which was classified as problematic, has been found in MuYuCMS 2.2. This issue affects some unknown processing of the file index.php. The manipulation of the argument file_path leads to path traversal. 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-221735. **CVE ID : CVE-2023-1002**	N/A	A-MUY-MUYU-160323/361
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Feb-2023	4.3	A vulnerability was found in MuYuCMS 2.2. It has been classified as problematic. Affected is an unknown function of the file /editor/index.php. The manipulation of the argument dir_path leads to	N/A	A-MUY-MUYU-160323/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			relative path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-221802 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1043**		
Vendor: mz-automation					
Product: lib60870					
Affected Version(s): 2.3.2					
Missing Release of Memory after Effective Lifetime	24-Feb-2023	5.5	An issue was discovered in lib60870 v2.3.2. There is a memory leak in lib60870/lib60870-C/examples/multi_client_server/multi_client_server.c. **CVE ID : CVE-2023-23205**	N/A	A-MZ--LIB6-160323/363
Vendor: Neo4j					
Product: awesome_procedures_on_cyper					
Affected Version(s): * Up to (excluding) 5.5.0					
Improper Restriction of XML External Entity Reference	16-Feb-2023	8.1	APOC (Awesome Procedures on Cypher) is an add-on library for Neo4j. An XML External Entity (XXE) vulnerability found in the apoc.import.graphml procedure of APOC core plugin prior to version 5.5.0 in	https://github.com/neo4j/apoc/pull/310, https://github.com/neo4j/apoc/security/advisories/GHSA-6wxg-wh7f-rqpr	A-NEO-AWES-160323/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Neo4j graph database. XML External Entity (XXE) injection occurs when the XML parser allows external entities to be resolved. The XML parser used by the apoc.import.graphml procedure was not configured in a secure way and therefore allowed this. External entities can be used to read local files, send HTTP requests, and perform denial-of-service attacks on the application. Abusing the XXE vulnerability enabled assessors to read local files remotely. Although with the level of privileges assessors had this was limited to one-line files. With the ability to write to the database, any file could have been read. Additionally, assessors noted, with local testing, the server could be crashed by passing in improperly formatted XML. The minimum version containing a patch for this vulnerability is 5.5.0. Those who		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cannot upgrade the library can control the allowlist of the procedures that can be used in your system. **CVE ID : CVE-2023-23926**		
Vendor: nethack					
Product: nethack					
Affected Version(s): From (including) 3.6.2 Up to (excluding) 3.6.7					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Feb-2023	5.5	NetHack is a single player dungeon exploration game. Starting with version 3.6.2 and prior to version 3.6.7, illegal input to the "C" (call) command can cause a buffer overflow and crash the NetHack process. This vulnerability may be a security issue for systems that have NetHack installed suid/sgid and for shared systems. For all systems, it may result in a process crash. This issue is resolved in NetHack 3.6.7. There are no known workarounds. **CVE ID : CVE-2023-24809**	https://github.com/NetHack/NetHack/security/advisories/GHSA-2cqv-5w4v-mgch, https://nethack.org/security/CVE-2023-24809.html	A-NET-NETH-160323/365
Vendor: netmodule					
Product: netmodule_router_software					
Affected Version(s): From (including) 4.3.0.0 Up to (excluding) 4.3.0.119					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	NetModule NSRW web administration interface executes an OS command constructed with unsanitized user input. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. **CVE ID : CVE-2023-0861**	N/A	A-NET-NETM-160323/366
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	8.8	The NetModule NSRW web administration interface is vulnerable to path traversals, which could lead to arbitrary file uploads and deletion. By uploading malicious files to the web root directory, authenticated users could gain remote command execution with elevated privileges. This issue affects NSRW: from 4.3.0.0 before	https://share.netmodule.com/public/system-software/4.7/4.7.0.103/NRSW-RN-4.7.0.103.pdf	A-NET-NETM-160323/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. **CVE ID : CVE-2023-0862**		
Affected Version(s): From (including) 4.4.0.0 Up to (excluding) 4.4.0.118					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	NetModule NSRW web administration interface executes an OS command constructed with unsanitized user input. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. **CVE ID : CVE-2023-0861**	N/A	A-NET-NETM-160323/368
Improper Limitation of a Pathname to a Restricted Directory	16-Feb-2023	8.8	The NetModule NSRW web administration interface is vulnerable to path traversals, which could lead to arbitrary file uploads	https://share.netmodule.com/public/system-software/4.7/4.7.0.103/NRSW-RN-4.7.0.103.pdf	A-NET-NETM-160323/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			and deletion. By uploading malicious files to the web root directory, authenticated users could gain remote command execution with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. **CVE ID : CVE-2023-0862**		
Affected Version(s): From (including) 4.6.0.0 Up to (excluding) 4.6.0.105					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	NetModule NSRW web administration interface executes an OS command constructed with unsanitized user input. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103.	N/A	A-NET-NETM-160323/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0861		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	8.8	The NetModule NSRW web administration interface is vulnerable to path traversals, which could lead to arbitrary file uploads and deletion. By uploading malicious files to the web root directory, authenticated users could gain remote command execution with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. **CVE ID : CVE-2023-0862**	https://share.netmodule.com/public/system-software/4.7/4.7.0.103/NRSW-RN-4.7.0.103.pdf	A-NET-NETM-160323/371
Affected Version(s): From (including) 4.7.0.0 Up to (excluding) 4.7.0.103					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Feb-2023	8.8	NetModule NSRW web administration interface executes an OS command constructed with unsanitized user input. A successful exploit could allow an authenticated user to execute arbitrary commands with elevated	N/A	A-NET-NETM-160323/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. **CVE ID : CVE-2023-0861**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Feb-2023	8.8	The NetModule NSRW web administration interface is vulnerable to path traversals, which could lead to arbitrary file uploads and deletion. By uploading malicious files to the web root directory, authenticated users could gain remote command execution with elevated privileges. This issue affects NSRW: from 4.3.0.0 before 4.3.0.119, from 4.4.0.0 before 4.4.0.118, from 4.6.0.0 before 4.6.0.105, from 4.7.0.0 before 4.7.0.103. **CVE ID : CVE-2023-0862**	https://share.netmodule.com/public/system-software/4.7/4.7.0.103/NRSW-RN-4.7.0.103.pdf	A-NET-NETM-160323/373
Vendor: networktocode					
Product: nautobot					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.5.7					
N/A	21-Feb-2023	9.8	Nautobot is a Network Source of Truth and Network Automation Platform. All users of Nautobot versions earlier than 1.5.7 are impacted by a remote code execution vulnerability. Nautobot did not properly sandbox Jinja2 template rendering. In Nautobot 1.5.7 has enabled sandboxed environments for the Jinja2 template engine used internally for template rendering for the following objects: `extras.ComputedField`, `extras.CustomLink`, `extras.ExportTemplate`, `extras.Secret`, `extras.Webhook`. While no active exploits of this vulnerability are known this change has been made as a preventative measure to protect against any potential remote code execution attacks utilizing maliciously crafted template code. This change	https://github.com/nautobot/nautobot/commit/d47f157e83b0c353bb2b697f911882c71cf90ca0, https://github.com/nautobot/nautobot/security/advisories/GHSA-8mfq-f5wj-vw5m	A-NET-NAUT-160323/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			forces the Jinja2 template engine to use a `SandboxedEnvironment` on all new installations of Nautobot. This addresses any potential unsafe code execution everywhere the helper function `nautobot.utilities.utils.render_jinja2` is called. Additionally, the documentation that had previously suggesting the direct use of `jinja2.Template` has been revised to suggest `render_jinja2`. Users are advised to upgrade to Nautobot 1.5.7 or newer. For users that are unable to upgrade to the latest release of Nautobot, you may add the following setting to your `nautobot_config.py` to apply the sandbox environment enforcement: `TEMPLATES[1]["OPTIONS"]["environment"] = "jinja2.sandbox.SandboxedEnvironment"` After applying this change, you must restart all Nautobot		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			services, including any Celery worker processes. **Note:** *Nautobot specifies two template engines by default, the first being “django” for the Django built-in template engine, and the second being “jinja” for the Jinja2 template engine. This recommended setting will update the second item in the list of template engines, which is the Jinja2 engine.* For users that are unable to immediately update their configuration such as if a Nautobot service restart is too disruptive to operations, access to provide custom Jinja2 template values may be mitigated using permissions to restrict “change” (write) actions to the affected object types listed in the first section. **Note:** *This solution is intended to be stopgap until you can successfully update your `nautobot_config.py` or upgrade your		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Nautobot instance to apply the sandboxed environment enforcement.* **CVE ID : CVE-2023-25657**		
Vendor: Nextcloud					
Product: nextcloud_server					
Affected Version(s): * Up to (excluding) 23.0.12					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Folder::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25579**	https://github.com/nextcloud/server/pull/35074, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-273v-9h7x-p68v	A-NEX-NEXT-160323/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 25.0.0					
N/A	25-Feb-2023	7.5	Nextcloud is an Open Source private cloud software. Versions 24.0.4 and above, prior to 24.0.7, and 25.0.0 and above, prior to 25.0.1, contain Improper Access Control. Secure view for internal shares can be circumvented if reshare permissions are also given. This issue is patched in versions 24.0.7 and 25.0.1. No workaround is available. **CVE ID : CVE-2023-25821**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-7w6h-5qgw-4j94, https://github.com/nextcloud/server/pull/34502	A-NEX-NEXT-160323/376
Affected Version(s): From (including) 20.0.0 Up to (excluding) 20.0.14					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Folder::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users	https://github.com/nextcloud/server/pull/35074, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-273v-9h7x-p68v	A-NEX-NEXT-160323/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25579**		
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.0.9					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Folder::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue.	https://github.com/nextcloud/server/pull/35074, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-273v-9h7x-p68v	A-NEX-NEXT-160323/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25579		
Affected Version(s): From (including) 22.2.0 Up to (excluding) 22.2.10					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Folder::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25579**	https://github.com/nextcloud/server/pull/35074, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-273v-9h7x-p68v	A-NEX-NEXT-160323/379
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.12					
Improper Limitation of a Pathname to a Restricted	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Folder::getFullPath()`	https://github.com/nextcloud/server/pull/35074, https://github.com/nextclou	A-NEX-NEXT-160323/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25579**	d/security-advisories/security/advisories/GHSA-273v-9h7x-p68v	
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In affected versions the `OC\Files\Node\Folder::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths	https://github.com/nextcloud/server/pull/35074, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-273v-9h7x-p68v	A-NEX-NEXT-160323/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25579**		
Affected Version(s): From (including) 24.0.4 Up to (excluding) 24.0.7					
N/A	25-Feb-2023	7.5	Nextcloud is an Open Source private cloud software. Versions 24.0.4 and above, prior to 24.0.7, and 25.0.0 and above, prior to 25.0.1, contain Improper Access Control. Secure view for internal shares can be circumvented if reshare permissions are also given. This issue is patched in versions 24.0.7 and 25.0.1. No workaround is available. **CVE ID : CVE-2023-25821**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-7w6h-5qgw-4j94, https://github.com/nextcloud/server/pull/34502	A-NEX-NEXT-160323/382
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.2					
Improper Limitation of a	22-Feb-2023	7.5	Nextcloud server is a self hosted home cloud product. In	https://github.com/nextcloud/server/pull	A-NEX-NEXT-160323/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			affected versions the `OC\Files\Node\Folder::getFullPath()` function was validating and normalizing the string in the wrong order. The function is used in the `newFile()` and `newFolder()` items, which may allow to creation of paths outside of ones own space and overwriting data from other users with crafted paths. This issue has been addressed in versions 25.0.2, 24.0.8, and 23.0.12. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25579**	/35074, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-273v-9h7x-p68v	
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.3					
Uncontrolled Resource Consumption	25-Feb-2023	6.5	Nextcloud is an Open Source private cloud software. Versions 25.0.0 and above, prior to 25.0.3, are subject to Uncontrolled Resource Consumption. A user can configure a very long password, consuming more resources on	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-53q2-cm29-7j83, https://github.com/nextcloud/server/pull/35965	A-NEX-NEXT-160323/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password validation than desired. This issue is patched in 25.0.3 No workaround is available. **CVE ID : CVE-2023-25816**		
Product: nextcloud_talk					
Affected Version(s): From (including) 15.0.0 Up to (excluding) 15.0.3					
Exposure of Resource to Wrong Sphere	27-Feb-2023	4.3	Nextcloud Talk is a fully on-premises audio/video and chat communication service. When cron jobs were misconfigured and therefore messages are not expired, the API would still return them while they were then hidden by the frontend code. It is recommended that the Nextcloud Talk is upgraded to 15.0.3. There are no workaround available. **CVE ID : CVE-2023-26041**	https://github.com/nextcloud/spreed/pull/8515, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-j53p-r755-v4jf	A-NEX-NEXT-160323/385
Vendor: nic					
Product: knot_resolver					
Affected Version(s): * Up to (excluding) 5.6.0					
Allocation of Resources Without Limits or Throttling	21-Feb-2023	7.5	Knot Resolver before 5.6.0 enables attackers to consume its resources, launching amplification attacks	https://www.knot-resolver.cz/2023-01-26-knot-resolver-5.6.0.html	A-NIC-KNOT-160323/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and potentially causing a denial of service. Specifically, a single client query may lead to a hundred TCP connection attempts if a DNS server closes connections without providing a response. **CVE ID : CVE-2023-26249**		
Vendor: Nodejs					
Product: node.js					
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.21.3					
Incorrect Authorization	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/api/permissions.html) feature in Node.js and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy. **CVE ID : CVE-2023-23918**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. **CVE ID : CVE-2023-23919**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/388
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. **CVE ID : CVE-2023-23920**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/389
Affected Version(s): From (including) 14.0.0 Up to (including) 14.14.0					
Incorrect Authorization	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1	https://nodejs.org/en/blog/vulnerability/february-2023-	A-NOD-NODE-160323/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/api/permissions.html) feature in Node.js and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy. **CVE ID : CVE-2023-23918**	security-releases/	
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. **CVE ID : CVE-2023-23919**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. **CVE ID : CVE-2023-23920**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/392
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.19.1					
Incorrect Authorization	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/api/permissions.html) feature in Node.js and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy. **CVE ID : CVE-2023-23918**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. **CVE ID : CVE-2023-23919**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/394
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Feb-2023	5.4	Undici is an HTTP/1.1 client for Node.js. Starting with version 2.0.0 and prior to version 5.19.1, the undici library does not protect `host` HTTP header from CRLF injection vulnerabilities. This issue is patched in Undici v5.19.1. As a workaround, sanitize the `headers.host` string before passing to undici. **CVE ID : CVE-2023-23936**	https://github.com/nodejs/undici/commit/a2eff05401358f6595138df963837c24348f2034, https://github.com/nodejs/undici/security/advisories/GHSA-5r9g-qh6m-jxff	A-NOD-NODE-160323/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. **CVE ID : CVE-2023-23920**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/396
Affected Version(s): From (including) 16.0.0 Up to (including) 16.12.0					
Incorrect Authorization	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/api/permissions.html) feature in Node.js and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy. **CVE ID : CVE-2023-23918**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. **CVE ID : CVE-2023-23919**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/398
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. **CVE ID : CVE-2023-23920**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/399
Affected Version(s): From (including) 18.0.0 Up to (excluding) 18.14.1					
Incorrect Authorization	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1	https://nodejs.org/en/blog/vulnerability/february-2023-	A-NOD-NODE-160323/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/api/permissions.html) feature in Node.js and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy. **CVE ID : CVE-2023-23918**	security-releases/	
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. **CVE ID : CVE-2023-23919**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Feb-2023	5.4	Undici is an HTTP/1.1 client for Node.js. Starting with version 2.0.0 and prior to version 5.19.1, the undici library does not protect `host` HTTP header from CRLF injection vulnerabilities. This issue is patched in Undici v5.19.1. As a workaround, sanitize the `headers.host` string before passing to undici. **CVE ID : CVE-2023-23936**	https://github.com/nodejs/undici/commit/a2eff05401358f6595138df963837c24348f2034, https://github.com/nodejs/undici/security/advisories/GHSA-5r9g-qh6m-jxff	A-NOD-NODE-160323/402
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. **CVE ID : CVE-2023-23920**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/403
Affected Version(s): From (including) 18.0.0 Up to (including) 18.11.0					
Incorrect Authorization	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			experimental Permissions (https://nodejs.org/api/permissions.html) feature in Node.js and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy. **CVE ID : CVE-2023-23918**		
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. **CVE ID : CVE-2023-23919**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. **CVE ID : CVE-2023-23920**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/406
Affected Version(s): From (including) 19.0.0 Up to (excluding) 19.2.0					
N/A	23-Feb-2023	7.5	A cryptographic vulnerability exists in Node.js <19.2.0, <18.14.1, <16.19.1, <14.21.3 that in some cases did does not clear the OpenSSL error stack after operations that may set it. This may lead to false positive errors during subsequent cryptographic operations that happen to be on the same thread. This in turn could be used to cause a denial of service. **CVE ID : CVE-2023-23919**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/407
Affected Version(s): From (including) 19.0.0 Up to (excluding) 19.6.1					
Incorrect Authorization	23-Feb-2023	7.5	A privilege escalation vulnerability exists in Node.js <19.6.1,	https://nodejs.org/en/blog/vulnerability/february-	A-NOD-NODE-160323/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/api/permissions.html) feature in Node.js and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy. **CVE ID : CVE-2023-23918**	2023-security-releases/	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Feb-2023	5.4	Undici is an HTTP/1.1 client for Node.js. Starting with version 2.0.0 and prior to version 5.19.1, the undici library does not protect `host` HTTP header from CRLF injection vulnerabilities. This issue is patched in Undici v5.19.1. As a workaround, sanitize the `headers.host` string before passing to undici. **CVE ID : CVE-2023-23936**	https://github.com/nodejs/undici/commit/a2eff05401358f6595138df963837c24348f2034, https://github.com/nodejs/undici/security/advisories/GHSA-5r9g-qh6m-jxff	A-NOD-NODE-160323/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges. **CVE ID : CVE-2023-23920**	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	A-NOD-NODE-160323/410
Product: undici					
Affected Version(s): * Up to (excluding) 5.19.1					
N/A	16-Feb-2023	7.5	Undici is an HTTP/1.1 client for Node.js. Prior to version 5.19.1, the `Headers.set()` and `Headers.append()` methods are vulnerable to Regular Expression Denial of Service (ReDoS) attacks when untrusted values are passed into the functions. This is due to the inefficient regular expression used to normalize the values in the `headerValueNormalize()` utility function. This vulnerability was patched in v5.19.1. No known workarounds are available.	https://github.com/nodejs/undici/security/advisories/GHSA-r6ch-mqf9-qc9w, https://github.com/nodejs/undici/commit/f2324e549943f0b0937b09fb1c0c16cc7c93abdf	A-NOD-UNDI-160323/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24807		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 5.19.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Feb-2023	5.4	Undici is an HTTP/1.1 client for Node.js. Starting with version 2.0.0 and prior to version 5.19.1, the undici library does not protect `host` HTTP header from CRLF injection vulnerabilities. This issue is patched in Undici v5.19.1. As a workaround, sanitize the `headers.host` string before passing to undici. **CVE ID : CVE-2023-23936**	https://github.com/nodejs/undici/commit/a2eff05401358f6595138df963837c24348f2034, https://github.com/nodejs/undici/security/advisories/GHSA-5r9g-qh6m-jxff	A-NOD-UNDI-160323/412
Vendor: notation-go_project					
Product: notation-go					
Affected Version(s): 0.7.0					
Allocation of Resources Without Limits or Throttling	20-Feb-2023	7.5	notation-go is a collection of libraries for supporting Notation sign, verify, push, and pull of oci artifacts. Prior to version 1.0.0-rc.3, notation-go users will find their application using excessive memory when verifying signatures. The application will be killed, and thus availability is impacted. The	https://github.com/notaryproject/notation-go/security/advisories/GHSA-87x9-7grx-m28v	A-NOT-NOTA-160323/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problem has been patched in the release v1.0.0-rc.3. Some workarounds are available. Users can review their own trust policy file and check if the identity string contains `=#`. Meanwhile, users should only put trusted certificates in their trust stores referenced by their own trust policy files, and make sure the `authenticity` validation is set to `enforce`. **CVE ID : CVE-2023-25656**		
Affected Version(s): 0.8.0					
Allocation of Resources Without Limits or Throttling	20-Feb-2023	7.5	notation-go is a collection of libraries for supporting Notation sign, verify, push, and pull of oci artifacts. Prior to version 1.0.0-rc.3, notation-go users will find their application using excessive memory when verifying signatures. The application will be killed, and thus availability is impacted. The problem has been patched in the release v1.0.0-rc.3. Some workarounds	https://github.com/notaryproject/notation-go/security/advisories/GHSA-87x9-7grx-m28v	A-NOT-NOTA-160323/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are available. Users can review their own trust policy file and check if the identity string contains `=#`. Meanwhile, users should only put trusted certificates in their trust stores referenced by their own trust policy files, and make sure the `authenticity` validation is set to `enforce`. **CVE ID : CVE-2023-25656**		
Affected Version(s): 0.9.0					
Allocation of Resources Without Limits or Throttling	20-Feb-2023	7.5	notation-go is a collection of libraries for supporting Notation sign, verify, push, and pull of oci artifacts. Prior to version 1.0.0-rc.3, notation-go users will find their application using excessive memory when verifying signatures. The application will be killed, and thus availability is impacted. The problem has been patched in the release v1.0.0-rc.3. Some workarounds are available. Users can review their own trust policy file and check if the identity	https://github.com/notaryproject/notation-go/security/advisories/GHSA-87x9-7grx-m28v	A-NOT-NOTA-160323/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			string contains `=#`. Meanwhile, users should only put trusted certificates in their trust stores referenced by their own trust policy files, and make sure the `authenticity` validation is set to `enforce`. **CVE ID : CVE-2023-25656**		
Vendor: notepad--_project					
Product: notepad--					
Affected Version(s): 1.22					
Improper Resource Shutdown or Release	18-Feb-2023	5.5	A vulnerability, which was classified as problematic, was found in cxasm notepad-- 1.22. This affects an unknown part of the component Directory Comparison Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The associated identifier of this vulnerability is VDB-221475. **CVE ID : CVE-2023-0909**	N/A	A-NOT-NOTE-160323/416
Vendor: nuxt					
Product: nuxt					
Affected Version(s): * Up to (excluding) 3.2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	6.1	Cross-site Scripting (XSS) - Generic in GitHub repository nuxt/framework prior to 3.2.1. **CVE ID : CVE-2023-0878**	https://github.com/nuxt/framework/commit/7aa35ff958eec0c7d071d3fcd481db57281dbcd9, https://huntr.dev/bounties/a892caf7-b8c2-4638-8cee-eb779d51066a	A-NUX-NUXT-160323/417
Vendor: olevmedia					
Product: olevmedia_shortcodes					
Affected Version(s): * Up to (including) 1.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	The Olevmedia Shortcodes WordPress plugin through 1.1.9 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-2023-0168**	N/A	A-OLE-OLEV-160323/418
Vendor: online_boat_reservation_system_project					
Product: online_boat_reservation_system					
Affected Version(s): 1.0					
Improper Neutralizat	24-Feb-2023	6.1	A vulnerability has been found in	N/A	A-ONL-ONLI-160323/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			SourceCodester Online Boat Reservation System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /boat/login.php of the component POST Parameter Handler. The manipulation of the argument un 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-221755. **CVE ID : CVE-2023-1030**		
Vendor: online_catering_reservation_system_project					
Product: online_catering_reservation_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Online Catering Reservation System 1.0. This affects an unknown part of the file /reservation/add_message.php of the component POST	N/A	A-ONL-ONLI-160323/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parameter Handler. The manipulation of the argument fullname leads to sql injection. 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-222003. **CVE ID : CVE-2023-1100**		
Vendor: online_eyewear_shop_project					
Product: online_eyewear_shop					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	8.8	A vulnerability classified as problematic was found in SourceCodester Online Eyewear Shop 1.0. Affected by this vulnerability is an unknown functionality of the file admin/?page=orders/view_order. The manipulation of the argument id 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	N/A	A-ONL-ONLI-160323/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-221635. **CVE ID : CVE-2023-0966**		
Vendor: online_graduate_tracer_system_project					
Product: online_graduate_tracer_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Feb-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Online Graduate Tracer System 1.0. Affected by this issue is some unknown functionality of the file tracking/admin/add_acc.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-221798 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1040**	N/A	A-ONL-ONLI-160323/422
Vendor: online_pet_shop_we_app_project					
Product: online_pet_shop_we_app					
Affected Version(s): 1.0					
Improper Neutralization of Input	26-Feb-2023	6.1	A vulnerability has been found in SourceCodester Online Pet Shop We	N/A	A-ONL-ONLI-160323/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			App 1.0 and classified as problematic. This vulnerability affects unknown code of the file /pet_shop/admin/orders/update_status.php. The manipulation of the argument oid with the input 1"><script>alert(1111)</script> leads to cross site scripting. 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-221800. **CVE ID : CVE-2023-1042**		
Vendor: online_pizza_ordering_system_project					
Product: online_pizza_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	9.8	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file /php-opos/index.php. The manipulation of the argument ID leads to sql injection. The attack can be	N/A	A-ONL-ONLI-160323/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221350 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0883**		
Missing Authentication for Critical Function	18-Feb-2023	9.8	A vulnerability classified as critical was found in SourceCodester Online Pizza Ordering System 1.0. Affected by this vulnerability is the function delete_category of the file ajax.php of the component POST Parameter Handler. The manipulation leads to missing authentication. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-221455. **CVE ID : CVE-2023-0906**	N/A	A-ONL-ONLI-160323/425
Improper Neutralization of Special Elements used in an SQL Command	18-Feb-2023	9.8	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the	N/A	A-ONL-ONLI-160323/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			file view_prod.php of the component GET Parameter Handler. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB-221476. **CVE ID : CVE-2023-0910**		
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	A vulnerability, which was classified as problematic, has been found in SourceCodester Online Pizza Ordering System 1.0. This issue affects some unknown processing of the file admin/ajax.php?action=save_user. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221681 was assigned to this vulnerability. **CVE ID : CVE-2023-0988**	N/A	A-ONL-ONLI-160323/427
Improper Neutralization of Input	23-Feb-2023	5.4	A vulnerability classified as problematic was found in	N/A	A-ONL-ONLI-160323/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			SourceCodester Online Pizza Ordering System 1.0. This vulnerability affects unknown code of the file index.php?page=checkout. The manipulation leads to cross site scripting. 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-221680. **CVE ID : CVE-2023-0987**		
Vendor: online_reviewer_management_system_project					
Product: online_reviewer_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Online Reviewer Management System 1.0. Affected is an unknown function of the file /reviewer_0/admins/assessments/pretest/questions-view.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely.	N/A	A-ONL-ONLI-160323/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221796. **CVE ID : CVE-2023-1038**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Feb-2023	7.2	An issue was discovered in Online Reviewer Management System v1.0. There is a SQL injection that can directly issue instructions to the background database system via reviewer_0/admins/assessments/course/course-update.php. **CVE ID : CVE-2023-25432**	N/A	A-ONL-ONLI-160323/430
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Feb-2023	4.8	An issue was discovered in Online Reviewer Management System v1.0. There is a XSS vulnerability via reviewer_0/admins/assessments/course/course-update.php. **CVE ID : CVE-2023-25431**	N/A	A-ONL-ONLI-160323/431
Vendor: online_services_project					
Product: online_services					
Affected Version(s): * Up to (excluding) 1.17					
Improper Neutralization of Special	23-Feb-2023	9.8	Improper Neutralization of Special Elements used in an SQL	N/A	A-ONL-ONLI-160323/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Command ('SQL Injection') vulnerability in NTN Information Technologies Online Services Software allows SQL Injection.This issue affects Online Services Software: before 1.17. **CVE ID : CVE-2023-0939**		
Vendor: online_student_management_system_project					
Product: online_student_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Feb-2023	9.8	A vulnerability was found in SourceCodester Online Student Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file eduauth/edit-class-detail.php. The manipulation of the argument editid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222002 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1099**	N/A	A-ONL-ONLI-160323/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Open-emr					
Product: openemr					
Affected Version(s): * Up to (excluding) 7.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	8.8	A Local File Inclusion (LFI) vulnerability in interface/forms/LBF/new.php in OpenEMR < 7.0.0 allows remote authenticated users to execute code via the formname parameter. **CVE ID : CVE-2023-22973**	https://www.open-emr.org/wiki/index.php/OpenEMR_Patches#7.0.0_Patch_.2811.2F30.2F22.29	A-OPE-OPEN-160323/434
Files or Directories Accessible to External Parties	22-Feb-2023	7.5	A Path Traversal in setup.php in OpenEMR < 7.0.0 allows remote unauthenticated users to read arbitrary files by controlling a connection to an attacker-controlled MySQL server. **CVE ID : CVE-2023-22974**	https://www.open-emr.org/wiki/index.php/OpenEMR_Patches#7.0.0_Patch_.2811.2F30.2F22.29	A-OPE-OPEN-160323/435
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	5.4	A Reflected Cross-site scripting (XSS) vulnerability in interface/forms/eye_mag/php/eye_mag_functions.php in OpenEMR < 7.0.0 allows remote authenticated users to inject arbitrary web script or HTML via the REQUEST_URI.	https://www.open-emr.org/wiki/index.php/OpenEMR_Patches#7.0.0_Patch_.2811.2F30.2F22.29	A-OPE-OPEN-160323/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22972		
Vendor: opencats					
Product: opencats					
Affected Version(s): 0.9.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Feb-2023	6.1	Improper neutralization of input during web page generation allows an unauthenticated attacker to submit malicious Javascript as the answer to a questionnaire which would then be executed when an authenticated user reviews the candidate's submission. This could be used to steal other users' cookies and force users to make actions without their knowledge. **CVE ID : CVE-2023-27293**	N/A	A-OPE-OPEN-160323/437
URL Redirection to Untrusted Site ('Open Redirect')	28-Feb-2023	5.4	An open redirect vulnerability exposes OpenCATS to template injection due to improper validation of user-supplied GET parameters. **CVE ID : CVE-2023-27292**	N/A	A-OPE-OPEN-160323/438
Improper Neutralizat	28-Feb-2023	5.4	Improper neutralization of	N/A	A-OPE-OPEN-160323/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			input during web page generation allows an authenticated attacker with access to a restricted account to submit malicious Javascript as the description for a calendar event, which would then be executed in other users' browsers if they browse to that event. This could result in stealing session tokens from users with higher permission levels or forcing users to make actions without their knowledge. **CVE ID : CVE-2023-27294**		
Cross-Site Request Forgery (CSRF)	28-Feb-2023	5.4	Cross-site request forgery is facilitated by OpenCATS failure to require CSRF tokens in POST requests. An attacker can exploit this issue by creating a dummy page that executes Javascript in an authenticated user's session when visited. **CVE ID : CVE-2023-27295**	N/A	A-OPE-OPEN-160323/440
Vendor: Opennms					
Product: horizon					
Affected Version(s): * Up to (excluding) 31.0.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	23-Feb-2023	6.5	Potential Insertion of Sensitive Information into Jetty Log Files in multiple versions of OpenNMS Meridian and Horizon could allow disclosure of usernames and passwords if the logging level is set to debug. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. 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. **CVE ID : CVE-2023-0815**	https://github.com/OpenNMS/opennms/pull/5741/files	A-OPE-HORI-160323/441
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Feb-2023	6.1	Unauthenticated, stored cross-site scripting in the display of alarm reduction keys in multiple versions of OpenNMS Horizon and Meridian could allow an attacker access to confidential session information. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4.	https://github.com/OpenNMS/opennms/pull/5506/files	A-OPE-HORI-160323/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-0846**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	Multiple stored and reflected cross-site scripting vulnerabilities in webapp jsp pages in multiple versions of OpenNMS Meridian and Horizon could allow an attacker access to confidential session information. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. 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. **CVE ID : CVE-2023-0867**	https://github.com/OpenNMS/opennms/pull/5765	A-OPE-HORI-160323/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	Reflected cross-site scripting in graph results in multiple versions of OpenNMS Meridian and Horizon could allow an attacker access to steal session cookies. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. 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. **CVE ID : CVE-2023-0868**	https://github.com/OpenNMS/opennms/pull/5740	A-OPE-HORI-160323/444
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	Cross-site scripting in outage/list.htm in multiple versions of OpenNMS Meridian and Horizon allows an attacker access to confidential session information. The solution is to upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4 or newer. Meridian and Horizon installation instructions state that they are intended for	https://github.com/OpenNMS/opennms/pull/5734	A-OPE-HORI-160323/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installation within an organization's private networks and should not be directly accessible from the Internet. **CVE ID : CVE-2023-0869**		
Product: meridian					
Affected Version(s): * Up to (excluding) 2023.1.0					
Insertion of Sensitive Information into Log File	23-Feb-2023	6.5	Potential Insertion of Sensitive Information into Jetty Log Files in multiple versions of OpenNMS Meridian and Horizon could allow disclosure of usernames and passwords if the logging level is set to debug. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. 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. **CVE ID : CVE-2023-0815**	https://github.com/OpenNMS/opennms/pull/5741/files	A-OPE-MERI-160323/446
Improper Neutralization of Input	22-Feb-2023	6.1	Unauthenticated, stored cross-site scripting in the display of alarm	https://github.com/OpenNMS/opennms/pull/5506/files	A-OPE-MERI-160323/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			reduction keys in multiple versions of OpenNMS Horizon and Meridian could allow an attacker access to confidential session information. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. 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. **CVE ID : CVE-2023-0846**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	Multiple stored and reflected cross-site scripting vulnerabilities in webapp jsp pages in multiple versions of OpenNMS Meridian and Horizon could allow an attacker access to confidential session information. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. Meridian and Horizon installation instructions state that they are	https://github.com/OpenNMS/opennms/pull/5765	A-OPE-MERI-160323/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intended for installation within an organization's private networks and should not be directly accessible from the Internet. **CVE ID : CVE-2023-0867**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	Reflected cross-site scripting in graph results in multiple versions of OpenNMS Meridian and Horizon could allow an attacker access to steal session cookies. Users should upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4. 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. **CVE ID : CVE-2023-0868**	https://github.com/OpenNMS/opennms/pull/5740	A-OPE-MERI-160323/449
Improper Neutralization of Input During Web Page Generation	23-Feb-2023	6.1	Cross-site scripting in outage/list.htm in multiple versions of OpenNMS Meridian and Horizon allows an attacker access to confidential session information. The	https://github.com/OpenNMS/opennms/pull/5734	A-OPE-MERI-160323/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			solution is to upgrade to Meridian 2023.1.0 or newer, or Horizon 31.0.4 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. **CVE ID : CVE-2023-0869**		
Vendor: osgeo					
Product: geonode					
Affected Version(s): * Up to (excluding) 4.0.3					
Improper Restriction of XML External Entity Reference	27-Feb-2023	6.5	GeoNode is an open source platform that facilitates the creation, sharing, and collaborative use of geospatial data. GeoNode is vulnerable to an XML External Entity (XXE) injection in the style upload functionality of GeoServer leading to Arbitrary File Read. This issue has been patched in version 4.0.3. **CVE ID : CVE-2023-26043**	https://github.com/GeoNode/geonode/commit/2fdfe919f299b21f1609bf898f9dcfde58770ac0	A-OSG-GEON-160323/451
Product: geoserver					
Affected Version(s): * Up to (excluding) 2.18.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode functions* setting to mitigate ``strEndsWith``, ``strStartsWith`` and ``PropertyIsLike `` misuse and enable the PostGIS DataStore *preparedStatements* setting to mitigate the ``FeatureId`` misuse.	https://github.com/geoserver/geoserver/security/advisories/GHSA-7g5f-wrx8-5ccf, https://github.com/geoserver/geoserver/commit/145a8af798590288d270b240235e89c8f0b62e1d	A-OSG-GEOS-160323/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25157		
Affected Version(s): From (including) 2.19.0 Up to (excluding) 2.19.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode functions* setting to mitigate ``strEndsWith``, ``strStartsWith`` and ``PropertyIsLike `` misuse and enable the PostGIS DataStore *preparedStatement	https://github.com/geoserver/geoserver/security/advisories/GHSA-7g5f-wrx8-5ccf, https://github.com/geoserver/geoserver/commit/145a8af798590288d270b240235e89c8f0b62e1d	A-OSG-GEOS-160323/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			s* setting to mitigate the ``FeatureId`` misuse. **CVE ID : CVE-2023-25157**		
Affected Version(s): From (including) 2.20.0 Up to (excluding) 2.20.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode functions* setting to mitigate ``strEndsWith``, ``strStartsWith`` and ``PropertyIsLike `` misuse and enable	https://github.com/geoserver/geoserver/security/advisories/GHSA-7g5f-wrx8-5ccf, https://github.com/geoserver/geoserver/commit/145a8af798590288d270b240235e89c8f0b62e1d	A-OSG-GEOS-160323/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the PostGIS DataStore *preparedStatements* setting to mitigate the ``FeatureId`` misuse. **CVE ID : CVE-2023-25157**		
Affected Version(s): From (including) 2.21.0 Up to (excluding) 2.21.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode functions* setting to mitigate ``strEndsWith``,	https://github.com/geoserver/geoserver/security/advisories/GHSA-7g5f-wrx8-5ccf, https://github.com/geoserver/geoserver/commit/145a8af798590288d270b240235e89c8f0b62e1d	A-OSG-GEOS-160323/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			``strStartsWith`` and ``PropertyIsLike `` misuse and enable the PostGIS DataStore *preparedStatements* setting to mitigate the ``FeatureId`` misuse. **CVE ID : CVE-2023-25157**		
Affected Version(s): From (including) 2.22.0 Up to (excluding) 2.22.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Feb-2023	9.8	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages. Users are advised to upgrade to either version 2.21.4, or version 2.22.2 to resolve this issue. Users unable to upgrade should disable the PostGIS Datastore *encode	https://github.com/geoserver/geoserver/security/advisories/GHSA-7g5f-wrx8-5ccf, https://github.com/geoserver/geoserver/commit/145a8af798590288d270b240235e89c8f0b62e1d	A-OSG-GEOS-160323/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functions* setting to mitigate ``strEndsWith``, ``strStartsWith`` and ``PropertyIsLike `` misuse and enable the PostGIS DataStore *preparedStatements* setting to mitigate the ``FeatureId`` misuse. **CVE ID : CVE-2023-25157**		
Vendor: part-db_project					
Product: part-db					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	6.1	Part-DB is an open source inventory management system for your electronic components. User input was found not being properly escaped, which allowed malicious users to inject arbitrary HTML into the pages. The Content-Security-Policy forbids inline and external scripts so it is not possible to execute JavaScript code, unless in combination with other vulnerabilities. There are no workarounds, please upgrade to Pat-DB 1.0.2 or later.	https://github.com/Part-DB/Part-DB-server/security/advisories/GHSA-9pmh-gmxx-rg2x, https://github.com/Part-DB/Part-DB-server/commit/5b7f44f4eaacad8a79bcedec32780e00d7347099	A-PAR-PART-160323/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26042		
Vendor: peazip_project					
Product: peazip					
Affected Version(s): 9.0.0					
Allocation of Resources Without Limits or Throttling	17-Feb-2023	5.5	An issue in Giorgio Tani peazip v.9.0.0 allows attackers to cause a denial of service via the End of Archive tag function of the peazip/pea UNPEA feature. **CVE ID : CVE-2023-24785**	N/A	A-PEA-PEAZ-160323/458
Vendor: pharmacy_management_system_project					
Product: pharmacy_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	19-Feb-2023	9.8	A vulnerability has been found in codeprojects Pharmacy Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file add.php of the component Avatar Image Handler. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221494 is the identifier assigned to this vulnerability.	N/A	A-PHA-PHAR-160323/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0918		
Vendor: PHP					
Product: php					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.28					
Allocation of Resources Without Limits or Throttling	16-Feb-2023	8.1	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, core path resolution function allocate buffer one byte too small. When resolving paths with lengths close to system MAXPATHLEN setting, this may lead to the byte after the allocated buffer being overwritten with NUL value, which might lead to unauthorized data access or modification. **CVE ID : CVE-2023-0568**	https://bugs.php.net/bug.php?id=81746	A-PHP-PHP-160323/460
Uncontrolled Resource Consumption	16-Feb-2023	7.5	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, excessive number of parts in HTTP form upload can cause high resource consumption and excessive number of log entries. This can cause denial of service on the affected server by	N/A	A-PHP-PHP-160323/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exhausting CPU resources or disk space. **CVE ID : CVE-2023-0662**		
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.16					
Allocation of Resources Without Limits or Throttling	16-Feb-2023	8.1	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, core path resolution function allocate buffer one byte too small. When resolving paths with lengths close to system MAXPATHLEN setting, this may lead to the byte after the allocated buffer being overwritten with NUL value, which might lead to unauthorized data access or modification. **CVE ID : CVE-2023-0568**	https://bugs.php.net/bug.php?id=81746	A-PHP-PHP-160323/462
Uncontrolled Resource Consumption	16-Feb-2023	7.5	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, excessive number of parts in HTTP form upload can cause high resource consumption and excessive number of log entries. This can cause denial of service on the	N/A	A-PHP-PHP-160323/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected server by exhausting CPU resources or disk space. **CVE ID : CVE-2023-0662**		
Affected Version(s): From (including) 8.2.0 Up to (excluding) 8.2.3					
Allocation of Resources Without Limits or Throttling	16-Feb-2023	8.1	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, core path resolution function allocate buffer one byte too small. When resolving paths with lengths close to system MAXPATHLEN setting, this may lead to the byte after the allocated buffer being overwritten with NUL value, which might lead to unauthorized data access or modification. **CVE ID : CVE-2023-0568**	https://bugs.php.net/bug.php?id=81746	A-PHP-PHP-160323/464
Uncontrolled Resource Consumption	16-Feb-2023	7.5	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, excessive number of parts in HTTP form upload can cause high resource consumption and excessive number of log entries. This can cause denial of	N/A	A-PHP-PHP-160323/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service on the affected server by exhausting CPU resources or disk space. **CVE ID : CVE-2023-0662**		
Vendor: php-saml-sp_project					
Product: php-saml-sp					
Affected Version(s): * Up to (excluding) 1.1.1					
Improper Restriction of XML External Entity Reference	21-Feb-2023	6.5	php-saml-sp before 1.1.1 and 2.x before 2.1.1 allows reading arbitrary files as the webserver user because resolving XML external entities was silently enabled via \LIBXML_DTDLOAD | \LIBXML_DTDATTR. **CVE ID : CVE-2023-26267**	https://git.sr.ht/~fkooman/php-saml-sp/log, https://git.sr.ht/~fkooman/php-saml-sp/commit/851f75b298a77e62d9022f1b170f662f5f7716d6	A-PHP-PHP--160323/466
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.1.1					
Improper Restriction of XML External Entity Reference	21-Feb-2023	6.5	php-saml-sp before 1.1.1 and 2.x before 2.1.1 allows reading arbitrary files as the webserver user because resolving XML external entities was silently enabled via \LIBXML_DTDLOAD | \LIBXML_DTDATTR. **CVE ID : CVE-2023-26267**	https://git.sr.ht/~fkooman/php-saml-sp/log, https://git.sr.ht/~fkooman/php-saml-sp/commit/851f75b298a77e62d9022f1b170f662f5f7716d6	A-PHP-PHP--160323/467
Vendor: Phpmyfaq					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: phpmyfaq					
Affected Version(s): * Up to (excluding) 3.1.11					
Misinterpretation of Input	17-Feb-2023	4.3	Misinterpretation of Input in GitHub repository thorsten/phpmyfaq prior to 3.1.11. **CVE ID : CVE-2023-0880**	https://github.com/thorsten/phpmyfaq/commit/a67dca41576834a1ddfee61b9e799b686b75d4fa, https://huntr.dev/bounties/14fc4841-0f5d-4e12-bf9e-1b60d2ac6a6c	A-PHP-PHPM-160323/468
Vendor: Pimcore					
Product: pimcore					
Affected Version(s): * Up to (excluding) 10.5.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.18. **CVE ID : CVE-2023-1067**	https://huntr.dev/bounties/31d17b34-f80d-49f2-86e7-97ae715cc045, https://github.com/pimcore/pimcore/commit/4b5733266d7d6aeb4f221a15e005db83fc198edf	A-PIM-PIMC-160323/469
Vendor: pixelfed					
Product: pixelfed					
Affected Version(s): * Up to (excluding) 0.11.4					
N/A	18-Feb-2023	5.3	Exposure of Sensitive Information to an	https://huntr.dev/bounties/0327b1b2-	A-PIX-PIXE-160323/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Unauthorized Actor in GitHub repository pixelfed/pixelfed prior to 0.11.4. **CVE ID : CVE-2023-0901**	6e7c-4154-a307-15f236571010, https://github.com/pixelfed/pixelfed/commit/5b5f5bc38ca9ba39d0b7dacc3813fb899f71ba57	
N/A	19-Feb-2023	5.3	Improper Authorization in GitHub repository pixelfed/pixelfed prior to 0.11.4. **CVE ID : CVE-2023-0914**	https://github.com/pixelfed/pixelfed/commit/ef56f92c3d77e9bafaa70c08b7c04d5a61b8d454, https://huntr.dev/bounties/54d5fd76-e038-4eda-9e03-d5e95e09c0ec	A-PIX-PIXE-160323/471
Vendor: premio					
Product: my_sticky_elements					
Affected Version(s): * Up to (excluding) 2.0.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	7.2	The My Sticky Elements WordPress plugin before 2.0.9 does not properly sanitise and escape a parameter before using it in a SQL statement when deleting messages, leading to a SQL injection exploitable by high privilege users such as admin **CVE ID : CVE-2023-0487**	N/A	A-PRE-MY_S-160323/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: PTC					
Product: kepware_server					
Affected Version(s): * Up to (including) 6.12					
Integer Overflow or Wraparound	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0754**	N/A	A-PTC-KEPW-160323/473
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0755**	N/A	A-PTC-KEPW-160323/474
Product: kepware_serverex					
Affected Version(s): * Up to (including) 6.12					
Integer Overflow or Wraparound	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code.	N/A	A-PTC-KEPW-160323/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0754		
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0755**	N/A	A-PTC-KEPW-160323/476
Product: thingworx_.net-sdk					
Affected Version(s): * Up to (including) 5.8.4.971					
Integer Overflow or Wraparound	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0754**	N/A	A-PTC-THIN-160323/477
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0755**	N/A	A-PTC-THIN-160323/478
Product: thingworx_edge_c-sdk					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.2.12.1052					
Integer Overflow or Wraparound	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0754**	N/A	A-PTC-THIN-160323/479
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0755**	N/A	A-PTC-THIN-160323/480
Product: thingworx_edge_microserver					
Affected Version(s): * Up to (including) 5.4.10.0					
Integer Overflow or Wraparound	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0754**	N/A	A-PTC-THIN-160323/481
Improper Validation	23-Feb-2023	9.8	The affected products are	N/A	A-PTC-THIN-160323/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0755**		
Product: thingworx_industrial_connectivity					
Affected Version(s): -					
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0755**	N/A	A-PTC-THIN-160323/483
Affected Version(s): *					
Integer Overflow or Wraparound	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0754**	N/A	A-PTC-THIN-160323/484
Product: thingworx_kepware_edge					
Affected Version(s): * Up to (including) 1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0754**	N/A	A-PTC-THIN-160323/485
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0755**	N/A	A-PTC-THIN-160323/486
Vendor: puzzle					
Product: liima					
Affected Version(s): * Up to (excluding) 1.17.28					
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	20-Feb-2023	9.8	Liima before 1.17.28 allows server-side template injection. **CVE ID : CVE-2023-26092**	https://github.com/liimaorg/liima/pull/678	A-PUZ-LIIM-160323/487
Improper Neutralizat	20-Feb-2023	9.8	Liima before 1.17.28 allows Hibernate	https://github.com/liimaorg	A-PUZ-LIIM-160323/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			query language (HQL) injection, related to colToSort in the deployment filter. **CVE ID : CVE-2023-26093**	/liima/pull/663	
Vendor: Python					
Product: python					
Affected Version(s): * Up to (excluding) 3.11					
Improper Input Validation	17-Feb-2023	7.5	An issue in the urllib.parse component of Python before v3.11 allows attackers to bypass blocklisting methods by supplying a URL that starts with blank characters. **CVE ID : CVE-2023-24329**	https://github.com/python/cpython/pull/99421	A-PYT-PYTH-160323/489
Vendor: quantumcloud					
Product: chatbot					
Affected Version(s): * Up to (excluding) 4.2.9					
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in QuantumCloud ChatBot ? plugin <= 4.2.8 versions. **CVE ID : CVE-2023-24415**	N/A	A-QUA-CHAT-160323/490
Vendor: quarkus					
Product: quarkus					
Affected Version(s): * Up to (excluding) 2.16.1					
Exposure of	24-Feb-2023	3.3	In RestEasy Reactive implementation of	https://github.com/quarkus	A-QUA-QUAR-160323/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			Quarkus the insecure File.createTempFile( ) is used in the FileBodyHandler class which creates temp files with insecure permissions that could be read by a local user. **CVE ID : CVE-2023-0481**	io/quarkus/pull/30694	
Affected Version(s): * Up to (excluding) 2.13.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Feb-2023	6.1	If the Quarkus Form Authentication session cookie Path attribute is set to `/` then a cross-site attack may be initiated which might lead to the Information Disclosure. This attack can be prevented with the Quarkus CSRF Prevention feature. **CVE ID : CVE-2023-0044**	N/A	A-QUA-QUAR-160323/492
Vendor: quick-plugins					
Product: loan_comparison					
Affected Version(s): * Up to (excluding) 1.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Loan Comparison WordPress plugin before 1.5.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode	N/A	A-QUI-LOAN-160323/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0366**		
Vendor: rangy_project					
Product: rangy					
Affected Version(s): -					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	24-Feb-2023	8.2	All versions of the package rangy are vulnerable to Prototype Pollution when using the extend() function in file rangy-core.js.The function uses recursive merge which can lead an attacker to modify properties of the Object.prototype **CVE ID : CVE-2023-26102**	N/A	A-RAN-RANG-160323/494
Vendor: read_more_excerpt_link_project					
Product: read_more_excerpt_link					
Affected Version(s): * Up to (including) 1.6.0					
Cross-Site Request Forgery (CSRF)	27-Feb-2023	4.3	The Download Read More Excerpt Link plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.6.0. This is due to missing or incorrect nonce validation on the	https://plugins.trac.wordpress.org/changeset/2871098/read-more-excerpt-link/trunk/read-more-excerpt-link.php	A-REA-READ-160323/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read_more_excerpt_link_menu_options() function. This makes it possible for unauthenticated attackers to update he plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1068**		
Vendor: realtimelogic					
Product: fuguhub					
Affected Version(s): * Up to (including) 8.1					
Improper Control of Generation of Code ('Code Injection')	17-Feb-2023	8.8	Real Time Logic FuguHub v8.1 and earlier was discovered to contain a remote code execution (RCE) vulnerability via the component /FuguHub/cmsdocs/ . **CVE ID : CVE-2023-24078**	N/A	A-REA-FUGU-160323/496
Vendor: Redhat					
Product: build_of_quarkus					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	23-Feb-2023	6.1	If the Quarkus Form Authentication session cookie Path attribute is set to `/` then a cross-site attack may be initiated which might	N/A	A-RED-BUIL-160323/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			lead to the Information Disclosure. This attack can be prevented with the Quarkus CSRF Prevention feature. **CVE ID : CVE-2023-0044**		
Product: directory_server					
Affected Version(s): 11.5					
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit-389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2023-1055**	https://bugzilla.redhat.com/show_bug.cgi?id=2173517#c0	A-RED-DIRE-160323/498
Affected Version(s): 11.6					
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword	https://bugzilla.redhat.com/show_bug.cgi?id=2173517#c0	A-RED-DIRE-160323/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit-389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2023-1055**		
Affected Version(s): 12.0					
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit-389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality.	https://bugzilla.redhat.com/show_bug.cgi?id=2173517#c0	A-RED-DIRE-160323/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1055		
Affected Version(s): 12.1					
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit-389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2023-1055**	https://bugzilla.redhat.com/show_bug.cgi?id=2173517#c0	A-RED-DIRE-160323/501
Product: resteasy					
Affected Version(s): * Up to (excluding) 4.7.8					
N/A	17-Feb-2023	5.5	In RESTEasy the insecure File.createTempFile() is used in the DataSourceProvider, FileProvider and Mime4JWorkaround classes which creates temp files with insecure permissions that could be read by a local user.	https://github.com/resteasy/resteasy/pull/3409/commits/807d7456f2137cde8ef7c316707211bf4e542d56	A-RED-REST-160323/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0482		
Vendor: rocket.chat					
Product: rocket.chat					
Affected Version(s): * Up to (excluding) 5.2.0					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	23-Feb-2023	8.8	A prototype pollution vulnerability exists in Rocket.Chat server <5.2.0 that could allow an attacker to a RCE under the admin account. Any user can create their own server in your cloud and become an admin so this vulnerability could affect the cloud infrastructure. This attack vector also may increase the impact of XSS to RCE which is dangerous for self-hosted users as well. **CVE ID : CVE-2023-23917**	N/A	A-ROC-ROCK-160323/503
Vendor: Rockwellautomation					
Product: kepserver_enterprise					
Affected Version(s): * Up to (including) 6.12					
Integer Overflow or Wraparound	23-Feb-2023	9.8	The affected products are vulnerable to an integer overflow or wraparound, which could allow an attacker to crash the server and remotely execute arbitrary code.	N/A	A-ROC-KEPS-160323/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0754		
Improper Validation of Array Index	23-Feb-2023	9.8	The affected products are vulnerable to an improper validation of array index, which could allow an attacker to crash the server and remotely execute arbitrary code. **CVE ID : CVE-2023-0755**	N/A	A-ROC-KEPS-160323/505
Vendor: rosariosis					
Product: rosariosis					
Affected Version(s): * Up to (excluding) 10.8.2					
Exposure of Sensitive Information to an Unauthorized Actor	24-Feb-2023	7.5	Improper Access Control in GitHub repository francoisjacquet/rosariosis prior to 10.8.2. **CVE ID : CVE-2023-0994**	https://github.com/francoisjacquet/rosariosis/commit/630d3e3d78270db8dbcbfe87db265bc3e70c5a76, https://huntr.dev/bounties/a281c586-9b97-4d17-88ff-ca91bb4c45ad	A-ROS-ROSA-160323/506
Vendor: salesagility					
Product: suitecrm					
Affected Version(s): * Up to (excluding) 7.12.9					
Path Traversal: '..filename'	25-Feb-2023	8.8	Path Traversal: '\..\filename' in GitHub repository salesagility/suitecrm prior to 7.12.9.	https://huntr.dev/bounties/0c1365bc-8d9a-4ae0-8b55-	A-SAL-SUIT-160323/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1034	615d492b3730, https://github.com/salesagility/suitecrm/commit/c19f221a41706efc8d73cef95c5e362c4f86bf06	
Vendor: sales_tracker_management_system_project					
Product: sales_tracker_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Sales Tracker Management System 1.0. Affected is an unknown function of the file admin/products/view_product.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. VDB-221634 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0964**	N/A	A-SAL-SALE-160323/508
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Feb-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Sales Tracker Management System 1.0. This affects an unknown part of the file admin/?page=user/manage_user of the	N/A	A-SAL-SALE-160323/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component Edit User. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-221679. **CVE ID : CVE-2023-0986**		
Cross-Site Request Forgery (CSRF)	24-Feb-2023	8.8	A vulnerability classified as problematic was found in SourceCodester Sales Tracker Management System 1.0. This vulnerability affects unknown code of the file admin/?page=user/list. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-221734 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0999**	N/A	A-SAL-SALE-160323/510
Vendor: sandhillsdev					
Product: easy_digital_downloads					
Affected Version(s): * Up to (excluding) 3.1.0.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Easy Digital Downloads WordPress plugin before 3.1.0.5 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0380**	N/A	A-SAN-EASY-160323/511
Vendor: Schneider-electric					
Product: clearscada					
Affected Version(s): *					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-CLEA-160323/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Product: ecostruxure_geo_scada_expert_2019					
Affected Version(s): -					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/513
Affected Version(s): 81.7268.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 81.7322.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0595		
Affected Version(s): 81.7429.2					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/516
Affected Version(s): 81.7457.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 81.7488.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/518
Affected Version(s): 81.7522.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/519
Affected Version(s): 81.7545.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019,	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 81.7578.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/521
Affected Version(s): 81.7613.1					
Improper Encoding or	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability	https://www.se.com/ww/en/download/document/SE	A-SCH-ECOS-160323/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	VD-2023-045-01/	
Affected Version(s): 81.7641.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 81.7690.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/524
Affected Version(s): 81.7714.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 81.7742.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0595		
Affected Version(s): 81.7777.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/527
Affected Version(s): 81.7808.2					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 81.7840.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/529
Affected Version(s): 81.7875.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/530
Affected Version(s): 81.7896.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019,	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 81.7936.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/532
Affected Version(s): 81.7980.1					
Improper Encoding or	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability	https://www.se.com/ww/en/download/document/SE	A-SCH-ECOS-160323/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	VD-2023-045-01/	
Affected Version(s): 81.8015.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 81.8108.2					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/535
Affected Version(s): 81.8122.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 81.8155.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0595		
Affected Version(s): 81.8172.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/538
Affected Version(s): 81.8197.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 81.8220.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/540
Affected Version(s): 81.8267.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/541
Product: ecostruxure_geo_scada_expert_2020					
Affected Version(s): -					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 83.7551.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/543
Affected Version(s): 83.7578.1					
Improper Encoding or	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for	https://www.se.com/ww/en/download/	A-SCH-ECOS-160323/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	document/SEVD-2023-045-01/	
Affected Version(s): 83.7613.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 83.7641.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/546
Affected Version(s): 83.7692.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 83.7717.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 83.7742.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/549
Affected Version(s): 83.7787.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 83.7809.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0595		
Affected Version(s): 83.7840.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/552
Affected Version(s): 83.7875.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 83.7913.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/554
Affected Version(s): 83.7936.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/555
Affected Version(s): 83.7980.2					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019,	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 83.8017.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/557
Affected Version(s): 83.8108.1					
Improper Encoding or	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability	https://www.se.com/ww/en/download/document/SE	A-SCH-ECOS-160323/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	VD-2023-045-01/	
Affected Version(s): 83.8122.2					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 83.8155.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/560
Affected Version(s): 83.8181.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 83.8197.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0595		
Affected Version(s): 83.8221.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/563
Affected Version(s): 83.8267.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Product: ecostruxure_geo_scada_expert_2021					
Affected Version(s): -					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 84.8027.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/566
Affected Version(s): 84.8108.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 84.8120.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/568
Affected Version(s): 84.8158.1					
Improper Encoding or	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for	https://www.se.com/ww/en/download/	A-SCH-ECOS-160323/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	document/SEVD-2023-045-01/	
Affected Version(s): 84.8182.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 84.8197.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/571
Affected Version(s): 84.8218.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Affected Version(s): 84.8269.1					
Improper Encoding or Escaping of Output	24-Feb-2023	5.3	A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October	https://www.se.com/ww/en/download/document/SEVD-2023-045-01/	A-SCH-ECOS-160323/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022), ClearSCADA (All Versions) **CVE ID : CVE-2023-0595**		
Vendor: seacms					
Product: seacms					
Affected Version(s): 11.6					
Deserialization of Untrusted Data	22-Feb-2023	9.8	A vulnerability was found in SeaCMS 11.6 and classified as problematic. Affected by this issue is some unknown functionality of the file /data/config.ftp.php of the component Picture Management. The manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-221630 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0960**	N/A	A-SEA-SEAC-160323/574
Vendor: sequelizejs					
Product: sequelize					
Affected Version(s): 7.0.0					
N/A	16-Feb-2023	9.8	Due to improper artibute filtering in the sequalize js library, can a	N/A	A-SEQ-SEQU-160323/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker peform SQL injections. **CVE ID : CVE-2023-22578**		
Access of Resource Using Incompatible Type ('Type Confusion')	16-Feb-2023	8.8	Due to improper parameter filtering in the sequalize js library, can a attacker peform injection. **CVE ID : CVE-2023-22579**	N/A	A-SEQ-SEQU-160323/576
Exposure of Sensitive Information to an Unauthorized Actor	16-Feb-2023	7.5	Due to improper input filtering in the sequalize js library, can malicious queries lead to sensitive information disclosure. **CVE ID : CVE-2023-22580**	N/A	A-SEQ-SEQU-160323/577
Affected Version(s): * Up to (excluding) 7.0.0					
Access of Resource Using Incompatible Type ('Type Confusion')	16-Feb-2023	8.8	Due to improper parameter filtering in the sequalize js library, can a attacker peform injection. **CVE ID : CVE-2023-22579**	N/A	A-SEQ-SEQU-160323/578
Exposure of Sensitive Information to an Unauthorized Actor	16-Feb-2023	7.5	Due to improper input filtering in the sequalize js library, can malicious queries lead to sensitive information disclosure. **CVE ID : CVE-2023-22580**	N/A	A-SEQ-SEQU-160323/579
Affected Version(s): * Up to (excluding) 6.19.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Feb-2023	9.8	Sequelize is a Node.js ORM tool. In versions prior to 6.19.1 a SQL injection exploit exists related to replacements. Parameters which are passed through replacements are not properly escaped which can lead to arbitrary SQL injection depending on the specific queries in use. The issue has been fixed in Sequelize 6.19.1. Users are advised to upgrade. Users unable to upgrade should not use the `replacements` and the `where` option in the same query. **CVE ID : CVE-2023-25813**	https://github.com/sequelize/sequelize/commit/ccaa3996047fe00048d5993ab2dd43ebadd4f78b, https://github.com/sequelize/sequelize/security/advisories/GHSA-wrh9-cjv3-2hpw	A-SEQ-SEQU-160323/580
Affected Version(s): * Up to (excluding) 6.29.0					
N/A	16-Feb-2023	9.8	Due to improper artibute filtering in the sequalize js library, can a attacker peform SQL injections. **CVE ID : CVE-2023-22578**	N/A	A-SEQ-SEQU-160323/581
Vendor: shortpixel					
Product: shortpixel_adaptive_images					
Affected Version(s): * Up to (excluding) 3.6.3					
Improper Neutralization of	27-Feb-2023	6.1	The ShortPixel Adaptive Images WordPress plugin	N/A	A-SHO-SHOR-160323/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			before 3.6.3 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 against any high privilege users such as admin **CVE ID : CVE-2023-0334**		
Vendor: simple_customer_relationship_management_system_project					
Product: simple_customer_relationship_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Feb-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Simple Customer Relationship Management System 1.0. This affects an unknown part of the file /php-scrm/login.php. The manipulation of the argument Password leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-221493 was assigned to this vulnerability. **CVE ID : CVE-2023-0917**	N/A	A-SIM-SIMP-160323/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter under the Admin Panel. **CVE ID : CVE-2023-24364**	N/A	A-SIM-SIMP-160323/584
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the Description parameter under the Create ticket function. **CVE ID : CVE-2023-24652**	N/A	A-SIM-SIMP-160323/585
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the oldpass parameter under the Change Password function. **CVE ID : CVE-2023-24653**	N/A	A-SIM-SIMP-160323/586
Improper Neutralization of Special Elements	27-Feb-2023	8.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL	N/A	A-SIM-SIMP-160323/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			injection vulnerability via the name parameter under the Request a Quote function. **CVE ID : CVE-2023-24654**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the subject parameter under the Create Ticket function. **CVE ID : CVE-2023-24656**	N/A	A-SIM-SIMP-160323/588
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the name parameter on the registration page. **CVE ID : CVE-2023-24651**	N/A	A-SIM-SIMP-160323/589
Vendor: simple_food_ordering_system_project					
Product: simple_food_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	18-Feb-2023	5.4	A vulnerability was found in SourceCodester Simple Food Ordering System 1.0. It has been classified as problematic. This affects an unknown	N/A	A-SIM-SIMP-160323/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			part of the file process_order.php. The manipulation of the argument order 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-221451. **CVE ID : CVE-2023-0902**		
Vendor: simple_responsive_tourism_website_project					
Product: simple_responsive_tourism_website					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Feb-2023	6.1	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Responsive Tourism Website 1.0. This affects an unknown part of the file /tourism/rate_review.php. The manipulation of the argument id with the input 1"><script>alert(1111)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the	N/A	A-SIM-SIMP-160323/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The associated identifier of this vulnerability is VDB-221799. **CVE ID : CVE-2023-1041**		
Vendor: smeup					
Product: erp					
Affected Version(s): tokyo_v6r1m220406					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Feb-2023	8.8	Sme.UP ERP TOKYO V6R1M220406 was discovered to contain an OS command injection vulnerability via calls made to the XMService component. **CVE ID : CVE-2023-26759**	N/A	A-SME-ERP-160323/592
Unrestricted Upload of File with Dangerous Type	27-Feb-2023	8.8	Sme.UP ERP TOKYO V6R1M220406 was discovered to contain an arbitrary file upload vulnerability. **CVE ID : CVE-2023-26762**	N/A	A-SME-ERP-160323/593
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Feb-2023	7.5	Sme.UP TOKYO V6R1M220406 was discovered to contain an arbitrary file download vulnerabilty via the component /ResourceService. **CVE ID : CVE-2023-26758**	N/A	A-SME-ERP-160323/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	27-Feb-2023	7.5	Sme.UP ERP TOKYO V6R1M220406 was discovered to contain an information disclosure vulnerability via the /debug endpoint. This vulnerability allows attackers to access cleartext credentials needed to authenticate to the AS400 system. **CVE ID : CVE-2023-26760**	N/A	A-SME-ERP-160323/595
Vendor: smg-webdesign					
Product: shortcode_for_font_awesome					
Affected Version(s): * Up to (excluding) 1.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Shortcode for Font Awesome WordPress plugin 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 embedded, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0419**	N/A	A-SMG-SHOR-160323/596
Vendor: snyk					
Product: kubernetes_monitor					
Affected Version(s): * Up to (excluding) 2.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	28-Feb-2023	5.3	This vulnerability in the Snyk Kubernetes Monitor can result in irrelevant data being posted to a Snyk Organization, which could in turn obfuscate other, relevant, security issues. It does not expose the user of the integration to any direct security risk and no user data can be leaked. To exploit the vulnerability the attacker does not need to be authenticated to Snyk but does need to know the target's Integration ID (which may or may not be the same as the Organization ID, although this is an unpredictable UUID in either case). **CVE ID : CVE-2023-1065**	https://github.com/snyk/kubernetes-monitor/pull/1275, https://github.com/snyk/kubernetes-monitor/commit/5b9a7821680bbfb6c4a900ab05d898ce2b2cc157, https://snyk.io/blog/api-auth-vuln-snyk-kubernetes-cve-2023-1065/	A-SNY-KUBE-160323/597
Vendor: Spip					
Product: spip					
Affected Version(s): * Up to (excluding) 3.2.18					
N/A	28-Feb-2023	9.8	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are	https://git.spip.net/spip/spip/commit/5aedf49b89415a4df3eb775eee3801a2b4b88266, https://git.spi	A-SPI-SPIP-160323/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.2.18, 4.0.10, 4.1.8, and 4.2.1. **CVE ID : CVE-2023-27372**	p.net/spip/spip/commit/96fbeb38711c6706e62457f2b732a652a04a409d	
Affected Version(s): * Up to (including) 4.1.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	9.8	SPIP v4.1.5 and earlier was discovered to contain a SQL injection vulnerability via the _oups parameter. This vulnerability allows attackers to execute arbitrary code via a crafted POST request. **CVE ID : CVE-2023-24258**	N/A	A-SPI-SPIP-160323/599
Affected Version(s): 4.2.0					
N/A	28-Feb-2023	9.8	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1. **CVE ID : CVE-2023-27372**	https://git.spip.net/spip/spip/commit/5aedf49b89415a4df3eb775eee3801a2b4b88266, https://git.spip.net/spip/spip/commit/96fbeb38711c6706e62457f2b732a652a04a409d	A-SPI-SPIP-160323/600
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.10					
N/A	28-Feb-2023	9.8	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because	https://git.spip.net/spip/spip/commit/5aedf49b89415a4df3eb775eee	A-SPI-SPIP-160323/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1. **CVE ID : CVE-2023-27372**	3801a2b4b88266, https://git.spip.net/spip/spip/commit/96fbeb38711c6706e62457f2b732a652a04a409d	
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.8					
N/A	28-Feb-2023	9.8	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1. **CVE ID : CVE-2023-27372**	https://git.spip.net/spip/spip/commit/5aedf49b89415a4df3eb775eee3801a2b4b88266, https://git.spip.net/spip/spip/commit/96fbeb38711c6706e62457f2b732a652a04a409d	A-SPI-SPIP-160323/602
Vendor: ss-proj					
Product: shirasagi					
Affected Version(s): * Up to (including) 1.16.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Feb-2023	5.4	Stored cross-site scripting vulnerability in Schedule function of SHIRASAGI v1.16.2 and earlier versions allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22425**	https://www.ss-proj.org/support/938.html	A-SS--SHIR-160323/603
Improper Neutralizat	24-Feb-2023	4.8	Stored cross-site scripting	https://www.ss-	A-SS--SHIR-160323/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Theme switching function of SHIRASAGI v1.16.2 and earlier versions allows a remote attacker with an administrative privilege to inject an arbitrary script. **CVE ID : CVE-2023-22427**	proj.org/support/938.html	
Vendor: stagil					
Product: stagil_navigation					
Affected Version(s): * Up to (excluding) 2.0.52					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.5	An unauthenticated path traversal vulnerability affects the "STAGIL Navigation for Jira - Menu & Themes" plugin before 2.0.52 for Jira. By modifying the fileName parameter to the snjCustomDesignConfig endpoint, it is possible to traverse and read the file system. **CVE ID : CVE-2023-26255**	N/A	A-STA-STAG-160323/605
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.5	An unauthenticated path traversal vulnerability affects the "STAGIL Navigation for Jira - Menu & Themes" plugin before 2.0.52 for Jira. By modifying the fileName parameter to the	N/A	A-STA-STAG-160323/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			snjFooterNavigation Config endpoint, it is possible to traverse and read the file system. **CVE ID : CVE-2023-26256**		
Vendor: strategy11					
Product: formidable_form_builder					
Affected Version(s): * Up to (excluding) 5.5.7					
Cross-Site Request Forgery (CSRF)	28-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Strategy11 Form Builder Team Formidable Forms plugin <= 5.5.6 versions. **CVE ID : CVE-2023-24419**	N/A	A-STR-FORM-160323/607
Vendor: struktur					
Product: libheif					
Affected Version(s): 1.14.2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-Feb-2023	7.8	There is a vulnerability in the strided image data parsing code in the emscripten wrapper for libheif. An attacker could exploit this through a crafted image file to cause a buffer overflow in linear memory during a memcpy call. **CVE ID : CVE-2023-0996**	https://github.com/strukturag/libheif/pull/759	A-STR-LIBH-160323/608
Vendor: sudo_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sudo					
Affected Version(s): * Up to (excluding) 1.9.13					
Double Free	28-Feb-2023	7.2	Sudo before 1.9.13p2 has a double free in the per-command chroot feature. **CVE ID : CVE-2023-27320**	N/A	A-SUD-SUDO-160323/609
Affected Version(s): 1.9.13					
Double Free	28-Feb-2023	7.2	Sudo before 1.9.13p2 has a double free in the per-command chroot feature. **CVE ID : CVE-2023-27320**	N/A	A-SUD-SUDO-160323/610
Vendor: Teampass					
Product: teampass					
Affected Version(s): * Up to (excluding) 3.0.0.22					
External Control of File Name or Path	27-Feb-2023	7.1	External Control of File Name or Path in GitHub repository nilsteampassnet/teampass prior to 3.0.0.22. **CVE ID : CVE-2023-1070**	https://huntr.dev/bounties/318bfdc4-7782-4979-956f-9ba2cc44889c, https://github.com/nilsteampassnet/teampass/commit/0af3574caba27a61b16dc25c94fa51ae12d2d967	A-TEA-TEAM-160323/611
Vendor: techpowerup					
Product: dram_calculator_for_ryzen					
Affected Version(s): 1.7.3					
Improper Initialization	26-Feb-2023	7.8	A vulnerability, which was classified as critical, has been	N/A	A-TEC-DRAM-160323/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			found in TechPowerUp Ryzen DRAM Calculator 1.2.0.5. This issue affects some unknown processing in the library WinRing0x64.sys. The manipulation leads to improper initialization. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221807. **CVE ID : CVE-2023-1048**		
Product: realtemp					
Affected Version(s): 3.7.0.0					
Improper Initialization	26-Feb-2023	7.8	A vulnerability classified as critical was found in TechPowerUp RealTemp 3.7.0.0. This vulnerability affects unknown code in the library WinRing0x64.sys. The manipulation leads to improper initialization. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. VDB-221806 is the identifier	https://github.com/zeze-zeze/WindowsKernelVuln/tree/master/CVE-2023-1047	A-TEC-REAL-160323/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-1047**		
Vendor: tftpd64_project					
Product: tftpd64					
Affected Version(s): 4.64					
Unquoted Search Path or Element	17-Feb-2023	7.8	A vulnerability was found in phjounin TFTPD64-SE 4.64 and classified as critical. This issue affects some unknown processing of the file tftpd64_svc.exe. The manipulation leads to unquoted search path. An attack has to be approached locally. The associated identifier of this vulnerability is VDB-221351. **CVE ID : CVE-2023-0887**	N/A	A-TFT-TFTP-160323/614
Vendor: themekraft					
Product: buddyforms					
Affected Version(s): * Up to (excluding) 2.7.8					
Deserialization of Untrusted Data	23-Feb-2023	9.8	The BuddyForms WordPress plugin, in versions prior to 2.7.8, was affected by an unauthenticated insecure deserialization issue. An unauthenticated attacker could leverage this issue to call files using a PHAR wrapper that	N/A	A-THE-BUDD-160323/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will deserialize the data and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. **CVE ID : CVE-2023-26326**		
Vendor: thingsboard					
Product: thingsboard					
Affected Version(s): 3.4.1					
Use of Hard-coded Credentials	23-Feb-2023	9.8	ThingsBoard 3.4.1 could allow a remote attacker to gain elevated privileges because hard-coded service credentials (usable for privilege escalation) are stored in an insecure format. (To read this stored data, the attacker needs access to the application server or its source code.) **CVE ID : CVE-2023-26462**	N/A	A-THI-THIN-160323/616
Vendor: Tibco					
Product: businessconnect					
Affected Version(s): * Up to (excluding) 7.3.1					
Improper Neutralization of Input During Web Page Generation	22-Feb-2023	5.4	The BusinessConnect UI component of TIBCO Software Inc.'s TIBCO BusinessConnect contains easily exploitable Reflected	https://www.tibco.com/services/support/advisories	A-TIB-BUSI-160323/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker with network access to execute scripts targeting the affected system or the victim's local system. Affected releases are TIBCO Software Inc.'s TIBCO BusinessConnect: versions 7.3.0 and below. **CVE ID : CVE-2023-26214**		
Vendor: timed_content_project					
Product: timed_content					
Affected Version(s): * Up to (excluding) 2.73					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The Timed Content WordPress plugin before 2.73 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-2023-0067**	N/A	A-TIM-TIME-160323/618
Vendor: tri					
Product: gigpress					
Affected Version(s): * Up to (including) 2.3.28					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	8.8	The GigPress WordPress plugin through 2.3.28 does not validate and escape some of its shortcode attributes before using them in SQL statement/s, which could allow any authenticated users, such as subscriber to perform SQL Injection attacks **CVE ID : CVE-2023-0381**	N/A	A-TRI-GIGP-160323/619
Vendor: trustedcomputinggroup					
Product: trusted_platform_module					
Affected Version(s): 2.0					
Out-of-bounds Write	28-Feb-2023	7.8	An out-of-bounds write vulnerability exists in TPM2.0's Module Library allowing writing of a 2-byte data past the end of TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can lead to denial of service (crashing the TPM chip/process or rendering it unusable) and/or arbitrary code execution in the TPM context. **CVE ID : CVE-2023-1017**	https://trustedcomputinggroup.org/wp-content/uploads/TCGVRT0007-Advisory-FINAL.pdf, https://trustedcomputinggroup.org/about/security/	A-TRU-TRUS-160323/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	28-Feb-2023	5.5	An out-of-bounds read vulnerability exists in TPM2.0's Module Library allowing a 2-byte read past the end of a TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can read or access sensitive data stored in the TPM. **CVE ID : CVE-2023-1018**	https://trustedcomputinggroup.org/wp-content/uploads/TCGVRT0007-Advisory-FINAL.pdf, https://trustedcomputinggroup.org/about/security/	A-TRU-TRUS-160323/621
Vendor: typecho					
Product: typecho					
Affected Version(s): * Up to (excluding) 1.2.0					
N/A	22-Feb-2023	9.8	typecho 1.1/17.10.30 was discovered to contain a remote code execution (RCE) vulnerability via install.php. **CVE ID : CVE-2023-24114**	N/A	A-TYP-TYPE-160323/622
Vendor: ujcms					
Product: ujcms					
Affected Version(s): From (including) 4.1.3 Up to (excluding) 5.5.1					
Improper Neutralization of Input During Web Page Generation	17-Feb-2023	6.1	A cross-site scripting (XSS) vulnerability in UJCMS v4.1.3 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the URL	https://github.com/ujcms/ujcms/issues/3	A-UJC-UJCM-160323/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			parameter under the Add New Articles function. **CVE ID : CVE-2023-24369**		
Vendor: uptime-kuma_project					
Product: uptime-kuma					
Affected Version(s): * Up to (excluding) 1.20.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	Uptime Kuma is a self-hosted monitoring tool. In versions prior to 1.20.0 the Uptime Kuma status page allows a persistent XSS attack. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-25810**	N/A	A-UPT-UPTI-160323/624
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	Uptime Kuma is a self-hosted monitoring tool. In versions prior to 1.20.0 the Uptime Kuma `name` parameter allows a persistent XSS attack. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-25811**	N/A	A-UPT-UPTI-160323/625
Vendor: utilities_project					
Product: utilities					
Affected Version(s): * Up to (including) 1.0.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	28-Feb-2023	7.5	All versions of the package utilities are vulnerable to Prototype Pollution via the _mix function. **CVE ID : CVE-2023-26105**	N/A	A-UTI-UTIL-160323/626
Vendor: vektor-inc					
Product: vk_all_in_one_expansion_unit					
Affected Version(s): * Up to (excluding) 9.86.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Feb-2023	5.4	The VK All in One Expansion Unit WordPress plugin before 9.86.0.0 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0230**	N/A	A-VEK-VK_A-160323/627
Vendor: versionn_project					
Product: versionn					
Affected Version(s): * Up to (excluding) 1.1.0					
Improper Neutralization of Special Elements used in a Command ('Comman	20-Feb-2023	9.8	versionn, software for changing version information across multiple files, has a command injection vulnerability in all versions prior to version 1.1.0. This	https://github.com/commenthol/versionn/commit/2ca128823efe962b37f2698f0eb530c2b124842d	A-VER-VERS-160323/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			issue is patched in version 1.1.0. **CVE ID : CVE-2023-25805**		
Vendor: Vmware					
Product: carbon_black_app_control					
Affected Version(s): From (including) 8.7.0 Up to (excluding) 8.7.8					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	22-Feb-2023	7.2	VMware Carbon Black App Control 8.7.x prior to 8.7.8, 8.8.x prior to 8.8.6, and 8.9.x.prior to 8.9.4 contain an injection vulnerability. A malicious actor with privileged access to the App Control administration console may be able to use specially crafted input allowing access to the underlying server operating system. **CVE ID : CVE-2023-20858**	https://www.vmware.com/security/advisories/VMSA-2023-0004.html	A-VMW-CARB-160323/629
Affected Version(s): From (including) 8.8.0 Up to (excluding) 8.8.6					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	22-Feb-2023	7.2	VMware Carbon Black App Control 8.7.x prior to 8.7.8, 8.8.x prior to 8.8.6, and 8.9.x.prior to 8.9.4 contain an injection vulnerability. A malicious actor with privileged access to the App Control administration	https://www.vmware.com/security/advisories/VMSA-2023-0004.html	A-VMW-CARB-160323/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			console may be able to use specially crafted input allowing access to the underlying server operating system. **CVE ID : CVE-2023-20858**		
Affected Version(s): From (including) 8.9.0 Up to (excluding) 8.9.4					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	22-Feb-2023	7.2	VMware Carbon Black App Control 8.7.x prior to 8.7.8, 8.8.x prior to 8.8.6, and 8.9.x.prior to 8.9.4 contain an injection vulnerability. A malicious actor with privileged access to the App Control administration console may be able to use specially crafted input allowing access to the underlying server operating system. **CVE ID : CVE-2023-20858**	https://www.vmware.com/security/advisories/VMSA-2023-0004.html	A-VMW-CARB-160323/631
Product: vrealize_automation					
Affected Version(s): From (including) 8.0 Up to (excluding) 8.11.1					
Improper Restriction of XML External Entity Reference	22-Feb-2023	8.8	VMware vRealize Orchestrator contains an XML External Entity (XXE) vulnerability. A malicious actor, with non-administrative access to vRealize Orchestrator, may be	https://www.vmware.com/security/advisories/VMSA-2023-0005.html	A-VMW-VREA-160323/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to use specially crafted input to bypass XML parsing restrictions leading to access to sensitive information or possible escalation of privileges. **CVE ID : CVE-2023-20855**		
Product: vrealize_orchestrator					
Affected Version(s): From (including) 8.0 Up to (excluding) 8.11.1					
Improper Restriction of XML External Entity Reference	22-Feb-2023	8.8	VMware vRealize Orchestrator contains an XML External Entity (XXE) vulnerability. A malicious actor, with non-administrative access to vRealize Orchestrator, may be able to use specially crafted input to bypass XML parsing restrictions leading to access to sensitive information or possible escalation of privileges. **CVE ID : CVE-2023-20855**	https://www.vmware.com/security/advisories/VMSA-2023-0005.html	A-VMW-VREA-160323/633
Product: workspace_one_content					
Affected Version(s): * Up to (excluding) 23.02					
Missing Authentication for Critical Function	28-Feb-2023	6.8	VMware Workspace ONE Content contains a passcode bypass vulnerability. A malicious actor, with access to a users rooted device, may be able to	https://www.vmware.com/security/advisories/VMSA-2023-0006.html	A-VMW-WORK-160323/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass the VMware Workspace ONE Content passcode. **CVE ID : CVE-2023-20857**		
Vendor: vox2png_project					
Product: vox2png					
Affected Version(s): 1.0					
Heap-based Buffer Overflow	24-Feb-2023	5.5	A vulnerability classified as critical was found in vox2png 1.0. Affected by this vulnerability is an unknown functionality of the file vox2png.c. The manipulation leads to heap-based buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221743. **CVE ID : CVE-2023-1010**	https://github.com/10cksYiqiyinHangzhouTechnology/vox2png/blob/main/README.md	A-VOX-VOX2-160323/635
Vendor: wangeditor					
Product: wangeditor					
Affected Version(s): * Up to (including) 5.0					
Improper Neutralization of Input During Web Page Generation	27-Feb-2023	5.4	WangEditor v5 was discovered to contain a cross-site scripting (XSS) vulnerability via the	N/A	A-WAN-WANG-160323/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			component /dist/index.js. **CVE ID : CVE-2023-24251**		
Vendor: weintek					
Product: easybuilder_pro					
Affected Version(s): * Up to (excluding) 6.07.02.480					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.8	The listed versions for Weintek EasyBuilder Pro are vulnerable to a ZipSlip attack caused by decompiling a malicious project file. This may allow an attacker to gain control of the user's computer or gain access to sensitive data. **CVE ID : CVE-2023-0104**	N/A	A-WEI-EASY-160323/637
Affected Version(s): From (including) 6.08.01.190 Up to (excluding) 6.08.01.350					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Feb-2023	7.8	The listed versions for Weintek EasyBuilder Pro are vulnerable to a ZipSlip attack caused by decompiling a malicious project file. This may allow an attacker to gain control of the user's computer or gain access to sensitive data. **CVE ID : CVE-2023-0104**	N/A	A-WEI-EASY-160323/638
Vendor: wow-company					
Product: wp_coder					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.5.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	4.9	The WP Coder – add custom html, css and js code plugin for WordPress is vulnerable to time-based SQL Injection via the 'id' parameter in versions up to, and including, 2.5.3 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 administrative privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2023-0895**	https://plugins.trac.wordpress.org/changeset?old=2757782&old_path=wp-coder%2Ftrunk%2Fadmin%2Fpartials%2Finclude-data.php&new=&new_path=wp-coder%2Ftrunk%2Fadmin%2Fpartials%2Finclude-data.php	A-WOW-WP_C-160323/639
Vendor: wpdevart					
Product: booking_calendar					
Affected Version(s): * Up to (excluding) 3.2.4					
Cross-Site Request Forgery (CSRF)	17-Feb-2023	5.4	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Booking calendar, Appointment Booking System plugin <= 3.2.3	N/A	A-WPD-BOOK-160323/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions affects plugin forms actions (create, duplicate, edit, delete). **CVE ID : CVE-2023-24388**		
Product: organization_chart					
Affected Version(s): * Up to (including) 1.4.4					
Cross-Site Request Forgery (CSRF)	23-Feb-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WpDevArt Organization chart <= 1.4.4 versions. **CVE ID : CVE-2023-24384**	N/A	A-WPD-ORGA-160323/641
Product: responsive_vertical_icon_menu					
Affected Version(s): * Up to (excluding) 1.5.9					
Cross-Site Request Forgery (CSRF)	28-Feb-2023	5.4	Cross-Site Request Forgery (CSRF) vulnerability in wpdevart Responsive Vertical Icon Menu plugin <= 1.5.8 can lead to theme deletion. **CVE ID : CVE-2023-23983**	N/A	A-WPD-RESP-160323/642
Vendor: wpdeveloper					
Product: reviewx					
Affected Version(s): * Up to (excluding) 1.6.4					
Improper Neutralization of Special Elements used in an SQL Command	23-Feb-2023	8.8	The 'rx_export_review' action in the ReviewX WordPress Plugin version < 1.6.4, is affected by an authenticated SQL injection	N/A	A-WPD-REVI-160323/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			vulnerability in the 'filterValue' and 'selectedColumns' parameters. **CVE ID : CVE-2023-26325**		
Vendor: wpgeodirectory					
Product: geodirectory					
Affected Version(s): * Up to (excluding) 2.2.24					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Feb-2023	7.2	The GeoDirectory WordPress plugin before 2.2.24 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin. **CVE ID : CVE-2023-0278**	N/A	A-WPG-GEOD-160323/644
Vendor: wp_font_awesome_project					
Product: wp_font_awesome					
Affected Version(s): * Up to (excluding) 1.7.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	The WP Font Awesome WordPress plugin before 1.7.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embedded, which could allow users with the contributor role and above to perform Stored	N/A	A-WP_-WP_F-160323/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Scripting attacks. **CVE ID : CVE-2023-0271**		
Vendor: xoslab					
Product: easy_file_locker					
Affected Version(s): 2.2.0.184					
Improper Resource Shutdown or Release	18-Feb-2023	7.8	A vulnerability, which was classified as problematic, was found in Xoslab Easy File Locker 2.2.0.184. This affects the function MessageNotifyCallback in the library xlkfs.sys. The manipulation leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-221457 was assigned to this vulnerability. **CVE ID : CVE-2023-0908**	N/A	A-XOS-EASY-160323/646
Vendor: yoga_class_registration_system_project					
Product: yoga_class_registration_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL	23-Feb-2023	9.8	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0 and classified as critical. This issue affects	N/A	A-YOG-YOGA-160323/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			some unknown processing of the file admin/registrations /update_status.php of the component Status Update Handler. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-221675. **CVE ID : CVE-2023-0980**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Feb-2023	9.8	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0. It has been classified as critical. Affected is an unknown function of the component Delete User. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-221676. **CVE ID : CVE-2023-0981**	N/A	A-YOG-YOGA-160323/648
Improper Neutralization of Special Elements	23-Feb-2023	9.8	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0. It has	N/A	A-YOG-YOGA-160323/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			been declared as critical. Affected by this vulnerability is an unknown functionality of the component Add Class Entry. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB-221677 was assigned to this vulnerability. **CVE ID : CVE-2023-0982**		
Vendor: zetacomponenets					
Product: mvctools					
Affected Version(s): 2008-09-23					
N/A	22-Feb-2023	9.8	MvcTools 6d48cd6830fc1df1d8c9d61caa1805fd6a1b7737 was discovered to contain a code execution backdoor via the request package (requirements.txt). This vulnerability allows attackers to access sensitive user information and execute arbitrary code. **CVE ID : CVE-2023-24108**	N/A	A-ZET-MVCT-160323/650
Vendor: Zoneminder					
Product: Zoneminder					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.36.33					
Missing Authorization	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 are vulnerable to Unauthenticated Remote Code Execution via Missing Authorization. There are no permissions check on the snapshot action, which expects an id to fetch an existing monitor but can be passed an object to create a new one instead. TriggerOn ends up calling shell_exec using the supplied Id. This issue is fixed in This issue is fixed in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26035**	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-72rg-h4vf-29gr	A-ZON-ZONE-160323/651
Untrusted Search Path	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-h5m9-6jjc-cgmw	A-ZON-ZONE-160323/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a Local File Inclusion (Untrusted Search Path) vulnerability via /web/index.php. By controlling $view, any local file ending in .php can be executed. This is supposed to be mitigated by calling detaintPath, however dentaintPath does not properly sandbox the path. This can be exploited by constructing paths like "..././", which get replaced by "../". This issue is patched in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26036**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain an SQL Injection. The minTime and maxTime request parameters are not properly validated and could be used execute arbitrary SQL. This issue is	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-65jp-2hj3-3733	A-ZON-ZONE-160323/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26037**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	8.8	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 are affected by a SQL Injection vulnerability. The (blind) SQL Injection vulnerability is present within the `filter[Query][terms][0][attr]` query string parameter of the `/zm/index.php` endpoint. A user with the View or Edit permissions of Events may execute arbitrary SQL. The resulting impact can include unauthorized data access (and modification), authentication and/or authorization bypass, and remote code execution. **CVE ID : CVE-2023-26034**	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-222j-wh8m-xjrx	A-ZON-ZONE-160323/654
Improper Neutralization of Special Elements	25-Feb-2023	8.8	ZoneMinder is a free, open source Closed-circuit television software application for Linux which	https://github.com/ZoneMinder/zoneminder/security/advisories/GHS	A-ZON-ZONE-160323/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain an OS Command Injection via daemonControl() in (/web/api/app/Controller/HostController.php). Any authenticated user can construct an api command to execute any shell command as the web user. This issue is patched in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26039**	A-44q8-h2pw-cc9g	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	8.1	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain SQL Injection via malicious jason web token. The Username field of the JWT token was trusted when performing an SQL query to load the user. If an attacker could determine the HASH key used by ZoneMinder, they could generate a	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-6c72-q9mw-mwx9	A-ZON-ZONE-160323/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious JWT token and use it to execute arbitrary SQL. This issue is fixed in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26032**		
Untrusted Search Path	25-Feb-2023	6.5	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain a Local File Inclusion (Untrusted Search Path) vulnerability via web/ajax/modal.php, where an arbitrary php file path can be passed in the request and loaded. This issue is patched in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26038**	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-wrx3-r8c4-r24w	A-ZON-ZONE-160323/657
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Feb-2023	6.1	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 are vulnerable to Cross-site Scripting. Log entries can be	https://github.com/ZoneMinder/zoneminder/commit/57bf25d39f12d620693f26068b8441b4f3f0b6c0, https://github.com/ZoneMinder/zoneminder/security/a	A-ZON-ZONE-160323/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected into the database logs, containing a malicious referrer field. This is unescaped when viewing the logs in the web ui. This issue is patched in version 1.36.33. **CVE ID : CVE-2023-25825**	dvisories/GHSA-68vf-g4qm-jr6v	
Affected Version(s): From (including) 1.37.0 Up to (excluding) 1.37.33					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Feb-2023	6.1	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 are vulnerable to Cross-site Scripting. Log entries can be injected into the database logs, containing a malicious referrer field. This is unescaped when viewing the logs in the web ui. This issue is patched in version 1.36.33. **CVE ID : CVE-2023-25825**	https://github.com/ZoneMinder/zoneminder/commit/57bf25d39f12d620693f26068b8441b4f3f0b6c0, https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-68vf-g4qm-jr6v	A-ZON-ZONE-160323/659
Affected Version(s): From (including) 1.37.00 Up to (excluding) 1.37.33					
Missing Authorization	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed-circuit television software application	https://github.com/ZoneMinder/zoneminder/security/a	A-ZON-ZONE-160323/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 are vulnerable to Unauthenticated Remote Code Execution via Missing Authorization. There are no permissions check on the snapshot action, which expects an id to fetch an existing monitor but can be passed an object to create a new one instead. TriggerOn ends up calling shell_exec using the supplied Id. This issue is fixed in This issue is fixed in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26035**	dvisories/GHSA-72rg-h4vf-29gr	
Untrusted Search Path	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain a Local File Inclusion (Untrusted Search Path) vulnerability via /web/index.php. By	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-h5m9-6jjc-cgmw	A-ZON-ZONE-160323/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controlling $view, any local file ending in .php can be executed. This is supposed to be mitigated by calling detaintPath, however dentaintPath does not properly sandbox the path. This can be exploited by constructing paths like "..././", which get replaced by "../". This issue is patched in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26036**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	9.8	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain an SQL Injection. The minTime and maxTime request parameters are not properly validated and could be used execute arbitrary SQL. This issue is fixed in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26037**	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-65jp-2hj3-3733	A-ZON-ZONE-160323/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	8.8	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 are affected by a SQL Injection vulnerability. The (blind) SQL Injection vulnerability is present within the `filter[Query][terms][0][attr]` query string parameter of the `/zm/index.php` endpoint. A user with the View or Edit permissions of Events may execute arbitrary SQL. The resulting impact can include unauthorized data access (and modification), authentication and/or authorization bypass, and remote code execution. **CVE ID : CVE-2023-26034**	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-222j-wh8m-xjrx	A-ZON-ZONE-160323/663
Improper Neutralization of Special Elements used in an OS Command ('OS	25-Feb-2023	8.8	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-44q8-h2pw-cc9g	A-ZON-ZONE-160323/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			contain an OS Command Injection via daemonControl() in (/web/api/app/Controller/HostController.php). Any authenticated user can construct an api command to execute any shell command as the web user. This issue is patched in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26039**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Feb-2023	8.1	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain SQL Injection via malicious jason web token. The Username field of the JWT token was trusted when performing an SQL query to load the user. If an attacker could determine the HASH key used by ZoneMinder, they could generate a malicious JWT token and use it to execute arbitrary SQL. This issue is fixed in	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-6c72-q9mw-mwx9	A-ZON-ZONE-160323/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26032**		
Untrusted Search Path	25-Feb-2023	6.5	ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras. Versions prior to 1.36.33 and 1.37.33 contain a Local File Inclusion (Untrusted Search Path) vulnerability via web/ajax/modal.php, where an arbitrary php file path can be passed in the request and loaded. This issue is patched in versions 1.36.33 and 1.37.33. **CVE ID : CVE-2023-26038**	https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-wrx3-r8c4-r24w	A-ZON-ZONE-160323/666
Hardware					
Vendor: abus					
Product: tvip_20000-21150					
Affected Version(s): -					
N/A	27-Feb-2023	7.2	ABUS TVIP 20000-21150 devices allows remote attackers to execute arbitrary code via shell metacharacters in the /cgi-bin/mft/wireless_mft ap field.	N/A	H-ABU-TVIP-160323/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26609		
Vendor: Axis					
Product: 207w					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	** UNSUPPORTED WHEN ASSIGNED ** A Vulnerability was discovered in Axis 207W network camera. There is a reflected XSS vulnerability in the web administration portal, which allows an attacker to execute arbitrary JavaScript via URL. **CVE ID : CVE-2023-22984**	N/A	H-AXI-207W-160323/668
Vendor: Cisco					
Product: firepower_4100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_4110					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-	H-CIS-FIRE-160323/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**	bkpsky-H8FCQgsA	
Product: firepower_4112					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20015		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_4115					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_4120					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_4125					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_4140					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_4145					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-FIRE-160323/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**	Advisory/cisco-sa-nxfp-cmdinj-XXBZjtR	
Use of Insufficient	23-Feb-2023	6.5	A vulnerability in the backup configuration	https://sec.cloudapps.cisco.c	H-CIS-FIRE-160323/684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ly Random Values			feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials.	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20016		
Product: firepower_4150					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_9300_sm-24					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_9300_sm-36					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_9300_sm-40					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_9300_sm-44					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-	H-CIS-FIRE-160323/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**	cmdinj-XXBZjtR	
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-FIRE-160323/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**	/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	
Product: firepower_9300_sm-44_x_3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_9300_sm-48					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_9300_sm-56					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: firepower_9300_sm-56_x_3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-FIRE-160323/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-FIRE-160323/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: mds_9000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9132t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9134					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9140					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/707
Product: mds_9148					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/708
Product: mds_9148s					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-MDS_-160323/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	Advisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: mds_9148t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9216					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9216a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20050		
Product: mds_9216i					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/714
Product: mds_9222i					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/715
Product: mds_9250i					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-	H-CIS-MDS_-160323/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	cmdinject-euQVK9u	
Product: mds_9396s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9396t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9506					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mds_9509					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/721
Product: mds_9513					
Affected Version(s): -					
Improper Neutralization of Special	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-MDS_-160323/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: mds_9700					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9706					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9710					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: mds_9718					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-MDS_-160323/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_1000v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/727
Product: nexus_1000_virtual_edge					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/728
Product: nexus_3016					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-NEXU-160323/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	Advisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: nexus_3016q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3048					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3064					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3064-32t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20050		
Product: nexus_3064-t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/734
Product: nexus_3064-x					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/735
Product: nexus_3064t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-	H-CIS-NEXU-160323/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	cmdinject-euQVK9u	
Product: nexus_3064x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3100-v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3100-z					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nexus_3100v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/741
Product: nexus_31108pc-v					
Affected Version(s): -					
Improper Neutralization of Special	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-NEXU-160323/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: nexus_31108pv-v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_31108tc-v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_31128pq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3132c-z					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3132q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/747
Product: nexus_3132q-v					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/748
Product: nexus_3132q-x					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-NEXU-160323/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	Advisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: nexus_3132q-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3132q-x\/3132q-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3164q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3172					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20050		
Product: nexus_3172pq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/754
Product: nexus_3172pq-xl					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/755
Product: nexus_3172pq\/pq-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-	H-CIS-NEXU-160323/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	cmdinject-euQVK9u	
Product: nexus_3172tq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3172tq-32t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3172tq-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nexus_3232c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/761
Product: nexus_3232c_					
Affected Version(s): -					
Improper Neutralization of Special	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-NEXU-160323/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: nexus_3264c-e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3264q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3400					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3408-s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_34180yc					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/767
Product: nexus_34200yc-sm					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/768
Product: nexus_3432d-s					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-NEXU-160323/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	Advisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: nexus_3464c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3524					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3524-x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20050		
Product: nexus_3524-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/774
Product: nexus_3524-x\/xl					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/775
Product: nexus_3548					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-	H-CIS-NEXU-160323/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	cmdinject-euQVK9u	
Product: nexus_3548-x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3548-xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3548-x\/xl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_3600					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nexus_36180yc-r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/781
Product: nexus_3636c-r					
Affected Version(s): -					
Improper Neutralization of Special	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-NEXU-160323/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: nexus_5500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_5548p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_5548up					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_5596t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_5596up					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/787
Product: nexus_5600					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/788
Product: nexus_56128p					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-NEXU-160323/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	Advisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: nexus_5624q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_5648q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_5672up					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_5672up-16g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20050		
Product: nexus_5696q					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/794
Product: nexus_6000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/795
Product: nexus_6001					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-	H-CIS-NEXU-160323/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	cmdinject-euQVK9u	
Product: nexus_6001p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_6001t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_6004					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_6004x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nexus_7000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/801
Product: nexus_7004					
Affected Version(s): -					
Improper Neutralization of Special	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-NEXU-160323/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: nexus_7009					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_7010					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_7018					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_7700					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_7702					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/807
Product: nexus_7706					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/808
Product: nexus_7710					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-NEXU-160323/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	Advisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	
Product: nexus_7718					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_9000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Product: nexus_9000v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	H-CIS-NEXU-160323/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_92160yc-x					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_92300yc					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_92304qc					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_92348gc-x					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9236c					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9272q					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93108tc-ex					
Affected Version(s): -					
Missing Release of Memory	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP)	https://sec.cloudapps.cisco.com/security/c	H-CIS-NEXU-160323/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as	enter/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93108tc-ex-24					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93108tc-fx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20089		
Product: nexus_93108tc-fx-24					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93108tc-fx3p					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93120tx					
Affected Version(s): -					
Missing Release of Memory after	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-NEXU-160323/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In	Advisory/cisco-sa-aci-lldp-dos-ySCNZOpX	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93128tx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9316d-gx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nexus_93180lc-ex					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93180yc-ex					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93180yc-ex-24					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-	H-CIS-NEXU-160323/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this	dos-ySCNZOpX	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93180yc-fx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93180yc-fx-24					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93180yc-fx3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx	H-CIS-NEXU-160323/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**		
Product: nexus_93180yc-fx3s					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx	H-CIS-NEXU-160323/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**		
Product: nexus_93216tc-fx2					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93240yc-fx2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9332c					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9332d-gx2b					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9332pq					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93360yc-fx2					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9336c-fx2					
Affected Version(s): -					
Missing Release of Memory	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP)	https://sec.cloudapps.cisco.com/security/c	H-CIS-NEXU-160323/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as	enter/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9336c-fx2-e					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9336pq_aci_spine					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20089		
Product: nexus_9348d-gx2a					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9348gc-fxp					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_93600cd-gx					
Affected Version(s): -					
Missing Release of Memory after	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-NEXU-160323/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In	Advisory/cisco-sa-aci-lldp-dos-ySCNZOpX	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9364c					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9364c-gx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nexus_9364d-gx2a					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9372px					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9372px-e					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-	H-CIS-NEXU-160323/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this	dos-ySCNZOpX	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9372tx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9372tx-e					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9396px					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9396tx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9408					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9508					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: nexus_9808					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	H-CIS-NEXU-160323/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: ucs_6200					
Affected Version(s): -					
Improper Neutralization of	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100	https://sec.cloudapps.cisco.com/security/c	H-CIS-UCS_-160323/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**	enter/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-UCS_-160323/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20016		
Product: ucs_6248up					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-UCS_-160323/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-UCS_-160323/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: ucs_6296up					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-UCS_-160323/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-UCS_-160323/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: ucs_6300					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-UCS_-160323/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-UCS_-160323/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: ucs_6324					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-UCS_-160323/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-UCS_-160323/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: ucs_6332					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-	H-CIS-UCS_-160323/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**	cmdinj-XXBZjtR	
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-UCS_-160323/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**	/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	
Product: ucs_6332-16up					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-UCS_-160323/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-UCS_-160323/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: ucs_64108					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-UCS_-160323/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-UCS_-160323/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx	H-CIS-UCS_-160323/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**		
Product: ucs_6454					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-UCS_-160323/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-UCS_-160323/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx	H-CIS-UCS_-160323/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**		
Product: ucs_6536					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	H-CIS-UCS_-160323/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	H-CIS-UCS_-160323/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx	H-CIS-UCS_-160323/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**		
Vendor: Dell					
Product: a200					
Affected Version(s): -					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	H-DEL-A200-160323/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Product: a2000					
Affected Version(s): -					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	H-DEL-A200-160323/885
Product: f800					
Affected Version(s): -					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-	H-DEL-F800-160323/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	multiple-security	
Product: f810					
Affected Version(s): -					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	H-DEL-F810-160323/887
Product: h400					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	H-DEL-H400-160323/888
Product: h500					
Affected Version(s): -					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	H-DEL-H500-160323/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Product: h5600					
Affected Version(s): -					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	H-DEL-H560-160323/890
Product: h600					
Affected Version(s): -					
Uncontrolled Resource	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810	https://www.dell.com/support/kbdoc/en-us/00020989	H-DEL-H600-160323/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	5/dell-emc-powerscale-onefs-security-updates-for-multiple-security	
Vendor: Draytek					
Product: vigor2960					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Feb-2023	5.5	A vulnerability classified as problematic has been found in DrayTek Vigor 2960 1.5.1.4. Affected is the function sub_1DF14 of the file /cgi-bin/mainfunction.cgi. The manipulation of the argument option with the input /../etc/password leads to path traversal. The attack needs to be done within the local network. The exploit	N/A	H-DRA-VIGO-160323/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. VDB-221742 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1009**		
Vendor: H3C					
Product: a210-g					
Affected Version(s): -					
Improper Authentication	22-Feb-2023	9.8	An access control issue in H3C A210-G A210-GV100R005 allows attackers to authenticate without a password. **CVE ID : CVE-2023-24093**	N/A	H-H3C-A210-160323/893
Vendor: Korenix					
Product: jetwave_2111					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	H-KOR-JETW-160323/894
Improper Neutralization of Special Elements used in a	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via	N/A	H-KOR-JETW-160323/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			/goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**		
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/896
Product: jetwave_2111l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	H-KOR-JETW-160323/897
Improper Neutralization of Special Elements used in a Command ('Comman	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd	N/A	H-KOR-JETW-160323/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**		
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/899
Product: jetwave_2114					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	H-KOR-JETW-160323/900
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root.	N/A	H-KOR-JETW-160323/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23295		
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/902
Product: jetwave_2211c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	H-KOR-JETW-160323/903
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/905
Product: jetwave_2212g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	H-KOR-JETW-160323/906
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/907
Uncontrolled Resource	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series	N/A	H-KOR-JETW-160323/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**		
Product: jetwave_2212s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	H-KOR-JETW-160323/909
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/910
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via	N/A	H-KOR-JETW-160323/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/formDefaul t. **CVE ID : CVE-2023-23296**		
Product: jetwave_2212x					
Affected Version(s): -					
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	H-KOR-JETW-160323/912
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCm d. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/913
Uncontroll ed Resource Consumpti on	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefaul t.	N/A	H-KOR-JETW-160323/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23296		
Product: jetwave_2411					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	H-KOR-JETW-160323/915
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/916
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/917
Product: jetwave_2411l					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	H-KOR-JETW-160323/918
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/919
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/920
Product: jetwave_2414					
Affected Version(s): -					
Improper Neutralizat	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and	N/A	H-KOR-JETW-160323/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/922
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/923
Product: jetwave_2460					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command	N/A	H-KOR-JETW-160323/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/925
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/926
Product: jetwave_3220_v3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter	N/A	H-KOR-JETW-160323/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			to execute commands as root. **CVE ID : CVE-2023-23294**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/928
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/929
Product: jetwave_3420_v3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root.	N/A	H-KOR-JETW-160323/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23294		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/931
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/932
Product: jetwave_4221hp-e					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	H-KOR-JETW-160323/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	H-KOR-JETW-160323/934
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	H-KOR-JETW-160323/935
Vendor: sick					
Product: fx0-gent00000					
Affected Version(s): -					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to	https://sick.com/psirt	H-SIC-FX0--160323/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the listener on TCP port 9000. **CVE ID : CVE-2023-23453**		
Product: fx0-gent00010					
Affected Version(s): -					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. **CVE ID : CVE-2023-23453**	https://sick.com/psirt	H-SIC-FX0--160323/937
Product: fx0-gpnt00000					
Affected Version(s): -					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000.	https://sick.com/psirt	H-SIC-FX0--160323/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23452		
Product: fx0-gpnt00010					
Affected Version(s): -					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. **CVE ID : CVE-2023-23452**	https://sick.com/psirt	H-SIC-FX0--160323/939
Vendor: Tenda					
Product: ac500					
Affected Version(s): -					
Out-of-bounds Write	27-Feb-2023	9.8	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromRouteStatic via parameters entrys and mitInterface. **CVE ID : CVE-2023-25233**	N/A	H-TEN-AC50-160323/940
Out-of-bounds Write	27-Feb-2023	9.8	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromAddressNat via parameters entrys and mitInterface.	N/A	H-TEN-AC50-160323/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25234		
Out-of-bounds Write	27-Feb-2023	7.5	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function formOneSsidCfgSet via parameter ssid. **CVE ID : CVE-2023-25235**	https://github.com/Fuzzy33/Vluninfo_Repo/tree/main/CNVDs/113_2	H-TEN-AC50-160323/942
Product: ax3					
Affected Version(s): -					
Out-of-bounds Write	23-Feb-2023	9.8	Tenda AX3 V16.03.12.11 was discovered to contain a stack overflow via the timeType function at /goform/SetSysTimeCfg. **CVE ID : CVE-2023-24212**	N/A	H-TEN-AX3-160323/943
Product: cp3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.2211041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS	N/A	H-TEN-CP3-160323/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tenda IT7-PRS<=V2209020908. **CVE ID : CVE-2023-23080**		
Product: cp7					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.2211041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7-PRS<=V2209020908. **CVE ID : CVE-2023-23080**	N/A	H-TEN-CP7-160323/945
Product: it7-lcs					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.2211041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-	N/A	H-TEN-IT7--160323/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7-PRS<=V2209020908. **CVE ID : CVE-2023-23080**		
Product: it7-pcs					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.2211041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7-PRS<=V2209020908. **CVE ID : CVE-2023-23080**	N/A	H-TEN-IT7--160323/947
Product: it7-prs					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.221	N/A	H-TEN-IT7--160323/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7-PRS<=V2209020908. **CVE ID : CVE-2023-23080**		
Product: w30e					
Affected Version(s): -					
Out-of-bounds Write	27-Feb-2023	9.8	Tenda Router W30E V1.0.1.25(633) is vulnerable to Buffer Overflow in function fromRouteStatic via parameters entrys and mitInterface. **CVE ID : CVE-2023-25231**	N/A	H-TEN-W30E-160323/949
Vendor: totolink					
Product: a7100ru					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Feb-2023	9.8	TOTOLink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability. **CVE ID : CVE-2023-24184**	N/A	H-TOT-A710-160323/950
Improper Neutralization of	16-Feb-2023	9.8	TOTOlink A7100RU(V7.4cu.2313_B20191024) was	N/A	H-TOT-A710-160323/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			discovered to contain a command injection vulnerability via the province parameter at setting/delStaticDhcpRules. **CVE ID : CVE-2023-24236**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Feb-2023	9.8	TOTOlink A7100RU(V7.4cu.2313_B20191024) was discovered to contain a command injection vulnerability via the city parameter at setting/delStaticDhcpRules. **CVE ID : CVE-2023-24238**	N/A	H-TOT-A710-160323/952
Product: a720r					
Affected Version(s): -					
Incorrect Authorization	17-Feb-2023	9.8	TOTOLINK A720R V4.1.5cu.532_B20210610 is vulnerable to Incorrect Access Control. **CVE ID : CVE-2023-23064**	N/A	H-TOT-A720-160323/953
Vendor: Tp-link					
Product: archer_c50					
Affected Version(s): 2					
Improper Resource Shutdown or Release	21-Feb-2023	6.5	A vulnerability was found in TP-Link Archer C50 V2_160801. It has been rated as	N/A	H-TP--ARCH-160323/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problematic. Affected by this issue is some unknown functionality of the component Web Management Interface. The manipulation leads to denial of service. The attack can only be initiated within the local network. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221552. **CVE ID : CVE-2023-0936**		
Product: tl-wr940n					
Affected Version(s): -					
Use of a Broken or Risky Cryptographic Algorithm	22-Feb-2023	7.5	TP-Link router TL-WR940N V6 3.19.1 Build 180119 uses a deprecated MD5 algorithm to hash the admin password used for basic authentication. **CVE ID : CVE-2023-23040**	https://midist0xf.medium.com/tl-wr940n-uses-weak-md5-hashing-algorithm-ae7b589860d2	H-TP--TL-W-160323/955
Vendor: ui					
Product: unifi_dream_machine_pro					
Affected Version(s): -					
N/A	23-Feb-2023	9.8	Ubiquiti Networks UniFi Dream Machine Pro v7.2.95 allows attackers to bypass domain	N/A	H-UI-UNIF-160323/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restrictions via crafted packets. **CVE ID : CVE-2023-24104**		
Vendor: Zyxel					
Product: lte3202-m437					
Affected Version(s): -					
N/A	21-Feb-2023	9.8	A security misconfiguration vulnerability exists in the Zyxel LTE3316-M604 firmware version V2.00(ABMP.6)C0 due to a factory default misconfiguration intended for testing purposes. A remote attacker could leverage this vulnerability to access an affected device using Telnet. **CVE ID : CVE-2023-22920**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-security-misconfiguration-vulnerability-of-4g-lte-indoor-routers	H-ZYX-LTE3-160323/957
Product: lte3316-m604					
Affected Version(s): -					
N/A	21-Feb-2023	9.8	A security misconfiguration vulnerability exists in the Zyxel LTE3316-M604 firmware version V2.00(ABMP.6)C0 due to a factory default misconfiguration intended for testing purposes. A remote attacker could	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-security-misconfiguration-vulnerability-of-4g-lte-	H-ZYX-LTE3-160323/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to access an affected device using Telnet. **CVE ID : CVE-2023-22920**	indoor-routers	
Operating System					
Vendor: abus					
Product: tvip_20000-21150_firmware					
Affected Version(s): -					
N/A	27-Feb-2023	7.2	ABUS TVIP 20000-21150 devices allows remote attackers to execute arbitrary code via shell metacharacters in the /cgi-bin/mft/wireless_mft ap field. **CVE ID : CVE-2023-26609**	N/A	O-ABU-TVIP-170323/959
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 15.7.3					
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://suppo	O-APP-IPAD-170323/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23504	rt.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2023-23500**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPAD-170323/961
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2,	https://support.apple.com/en-us/HT213598, https://suppo	O-APP-IPAD-170323/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23503**	rt.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. The quoted original message may be selected from the wrong email when forwarding an email from an Exchange account. **CVE ID : CVE-2023-23498**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606	O-APP-IPAD-170323/963
Insertion of Sensitive Information into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2,	https://support.apple.com/en-us/HT213598, https://support.apple.com/	O-APP-IPAD-170323/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. **CVE ID : CVE-2023-23505**	en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213599	
Affected Version(s): * Up to (excluding) 16.3					
N/A	27-Feb-2023	9.9	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. **CVE ID : CVE-2023-23531**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606	O-APP-IPAD-170323/965
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2,	https://support.apple.com/en-us/HT213605,	O-APP-IPAD-170323/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23496**	https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599, https://support.apple.com/en-us/HT213600	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23517**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601,	O-APP-IPAD-170323/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23518**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPAD-170323/968
N/A	27-Feb-2023	8.6	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606	O-APP-IPAD-170323/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			its sandbox or with certain elevated privileges. **CVE ID : CVE-2023-23530**		
Out-of-bounds Write	27-Feb-2023	7.5	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Processing an image may lead to a denial-of-service. **CVE ID : CVE-2023-23519**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPAD-170323/970
N/A	27-Feb-2023	6.5	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Visiting a website may lead to an app denial-of-service. **CVE ID : CVE-2023-23512**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPAD-170323/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	27-Feb-2023	5.9	A race condition was addressed with additional validation. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. A user may be able to read arbitrary files as root. **CVE ID : CVE-2023-23520**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606	O-APP-IPAD-170323/972
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access user-sensitive data. **CVE ID : CVE-2023-23499**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPAD-170323/973
N/A	27-Feb-2023	5.5	An information disclosure issue was	https://support.apple.com/	O-APP-IPAD-170323/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to determine kernel memory layout. **CVE ID : CVE-2023-23502**	en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23511**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/	O-APP-IPAD-170323/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213599	
Affected Version(s): * Up to (excluding) 16.3.1					
Access of Resource Using Incompatible Type ('Type Confusion')	27-Feb-2023	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, Safari 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2023-23529**	https://support.apple.com/en-us/HT213638, https://support.apple.com/en-us/HT213635, https://support.apple.com/en-us/HT213633	O-APP-IPAD-170323/976
Use After Free	27-Feb-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1. An app may be able to execute arbitrary code with kernel privileges.. **CVE ID : CVE-2023-23514**	https://support.apple.com/en-us/HT213635, https://support.apple.com/en-us/HT213633	O-APP-IPAD-170323/977
Uncontrolled Resource Consumption	27-Feb-2023	7.5	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS	https://support.apple.com/en-us/HT213634, https://suppo	O-APP-IPAD-170323/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of-service. **CVE ID : CVE-2023-23524**	rt.apple.com/en-us/HT213635, https://support.apple.com/en-us/HT213632, https://support.apple.com/en-us/HT213633	
Affected Version(s): From (including) 16.0 Up to (excluding) 16.3					
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-23504**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPAD-170323/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2023-23500**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPAD-170323/980
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23503**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601,	O-APP-IPAD-170323/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. The quoted original message may be selected from the wrong email when forwarding an email from an Exchange account. **CVE ID : CVE-2023-23498**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606	O-APP-IPAD-170323/982
Insertion of Sensitive Information into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. **CVE ID : CVE-2023-23505**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://suppo	O-APP-IPAD-170323/983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rt.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213599	
Product: iphone_os					
Affected Version(s): * Up to (excluding) 15.7.3					
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-23504**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPHO-170323/984
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue	https://support.apple.com/en-us/HT213598	O-APP-IPHO-170323/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2023-23500**	, https://support.apple.com/en-us/HT213605 , https://support.apple.com/en-us/HT213606 , https://support.apple.com/en-us/HT213601 , https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23503**	https://support.apple.com/en-us/HT213598 , https://support.apple.com/en-us/HT213605 , https://support.apple.com/en-us/HT213606 , https://support.apple.com/en-us/HT213601 , https://support.apple.com/	O-APP-IPHO-170323/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213599	
N/A	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. The quoted original message may be selected from the wrong email when forwarding an email from an Exchange account. **CVE ID : CVE-2023-23498**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606	O-APP-IPHO-170323/987
Insertion of Sensitive Information into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. **CVE ID : CVE-2023-23505**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-	O-APP-IPHO-170323/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213604 , https://support.apple.com/en-us/HT213599	
Affected Version(s): * Up to (excluding) 16.3					
N/A	27-Feb-2023	9.9	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. **CVE ID : CVE-2023-23531**	https://support.apple.com/en-us/HT213605 , https://support.apple.com/en-us/HT213606	O-APP-IPHO-170323/989
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23496**	https://support.apple.com/en-us/HT213605 , https://support.apple.com/en-us/HT213606 , https://support.apple.com/en-us/HT213601 , https://support.apple.com/en-us/HT213599 , https://suppo	O-APP-IPHO-170323/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rt.apple.com/en-us/HT213600	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23517**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPHO-170323/991
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://suppo	O-APP-IPHO-170323/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23518**	rt.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	8.6	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. **CVE ID : CVE-2023-23530**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606	O-APP-IPHO-170323/993
Out-of-bounds Write	27-Feb-2023	7.5	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3.	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606,	O-APP-IPHO-170323/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processing an image may lead to a denial-of-service. **CVE ID : CVE-2023-23519**	https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	6.5	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Visiting a website may lead to an app denial-of-service. **CVE ID : CVE-2023-23512**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPHO-170323/995
Time-of-check Time-of-use (TOCTOU) Race Condition	27-Feb-2023	5.9	A race condition was addressed with additional validation. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. A user may be able to read arbitrary files as root. **CVE ID : CVE-2023-23520**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606	O-APP-IPHO-170323/996
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened	https://support.apple.com/en-	O-APP-IPHO-170323/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access user-sensitive data. **CVE ID : CVE-2023-23499**	us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to determine kernel memory layout. **CVE ID : CVE-2023-23502**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-	O-APP-IPHO-170323/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213601 , https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23511**	https://support.apple.com/en-us/HT213605 , https://support.apple.com/en-us/HT213606 , https://support.apple.com/en-us/HT213604 , https://support.apple.com/en-us/HT213601 , https://support.apple.com/en-us/HT213599	O-APP-IPHO-170323/999
Affected Version(s): * Up to (excluding) 16.3.1					
Access of Resource Using Incompatible Type ('Type Confusion')	27-Feb-2023	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, Safari 16.3. Processing maliciously crafted web content may lead to arbitrary	https://support.apple.com/en-us/HT213638 , https://support.apple.com/en-us/HT213635 , https://support.apple.com/	O-APP-IPHO-170323/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2023-23529**	en-us/HT213633	
Use After Free	27-Feb-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1. An app may be able to execute arbitrary code with kernel privileges.. **CVE ID : CVE-2023-23514**	https://support.apple.com/en-us/HT213635, https://support.apple.com/en-us/HT213633	O-APP-IPHO-170323/1001
Uncontrolled Resource Consumption	27-Feb-2023	7.5	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of-service. **CVE ID : CVE-2023-23524**	https://support.apple.com/en-us/HT213634, https://support.apple.com/en-us/HT213635, https://support.apple.com/en-us/HT213632, https://support.apple.com/en-us/HT213633	O-APP-IPHO-170323/1002
Affected Version(s): From (including) 16.0 Up to (excluding) 16.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-23504**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPHO-170323/1003
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state.	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606,	O-APP-IPHO-170323/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23500	https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23503**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-IPHO-170323/1005
N/A	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. The quoted	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605,	O-APP-IPHO-170323/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			original message may be selected from the wrong email when forwarding an email from an Exchange account. **CVE ID : CVE-2023-23498**	https://support.apple.com/en-us/HT213606	
Insertion of Sensitive Information into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. **CVE ID : CVE-2023-23505**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213599	O-APP-IPHO-170323/1007
Product: macos					
Affected Version(s): -					
Improper Input Validation	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are	https://helpx.adobe.com/security/produc	O-APP-MACO-170323/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an Improper Input Validation 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-2023-21574**	ts/photoshop/apsb23-11.html	
Out-of-bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (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-2023-21575**	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	O-APP-MACO-170323/1009
Out-of-bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (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/photoshop/apsb23-11.html	O-APP-MACO-170323/1010

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-2023-21576**		
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by a Stack-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-2023-22226**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-APP-MACO-170323/1011
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-APP-MACO-170323/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-22227**		
Improper Input Validation	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an Improper Input Validation 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-2023-22228**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-APP-MACO-170323/1013
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-APP-MACO-170323/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22229		
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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-2023-22230**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-APP-MACO-170323/1015
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (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-2023-22236**	https://helpx.adobe.com/security/products/animate/apsb23-15.html	O-APP-MACO-170323/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (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-2023-22237**	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	O-APP-MACO-170323/1017
Out-of-bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (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-2023-22238**	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	O-APP-MACO-170323/1018
Improper Input Validation	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an Improper Input Validation vulnerability that	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	O-APP-MACO-170323/1019

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-2023-22239**		
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Stack-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-2023-22243**	https://helpx.adobe.com/security/products/animate/apsb23-15.html	O-APP-MACO-170323/1020
Use After Free	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (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/animate/apsb23-15.html	O-APP-MACO-170323/1021

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-2023-22246**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26. **CVE ID : CVE-2023-26020**	https://docs.craftercms.org/en/4.0/security/advisory.html#cv-2023021701	O-APP-MACO-170323/1022
Out-of-bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (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	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	O-APP-MACO-170323/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-21577**		
Out-of-bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (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-2023-21578**	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	O-APP-MACO-170323/1024
Out-of-bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-APP-MACO-170323/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-21583**		
NULL Pointer Dereference	17-Feb-2023	5.5	Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2023-21593**	https://helpx.adobe.com/security/products/indesign/apsb23-12.html	O-APP-MACO-170323/1026
Out-of-bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-APP-MACO-170323/1027

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-2023-22231**		
Out-of-bounds Read	17-Feb-2023	5.5	After Affects versions 23.1 (and earlier), 22.6.3 (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-2023-22233**	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	O-APP-MACO-170323/1028
Affected Version(s): * Up to (excluding) 11.7.3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Feb-2023	9.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604	O-APP-MACO-170323/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23513		
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23517**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1030
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/	O-APP-MACO-170323/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23518**	en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
Affected Version(s): * Up to (excluding) 13.2					
N/A	27-Feb-2023	9.9	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. **CVE ID : CVE-2023-23531**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606	O-APP-MACO-170323/1032
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606,	O-APP-MACO-170323/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23496**	https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599, https://support.apple.com/en-us/HT213600	
N/A	27-Feb-2023	8.6	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges. **CVE ID : CVE-2023-23530**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606	O-APP-MACO-170323/1034
Out-of-bounds Write	27-Feb-2023	7.5	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Processing an image may lead to a denial-of-service.	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601	O-APP-MACO-170323/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23519	, https://support.apple.com/en-us/HT213599	
Time-of-check Time-of-use (TOCTOU) Race Condition	27-Feb-2023	5.9	A race condition was addressed with additional validation. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. A user may be able to read arbitrary files as root. **CVE ID : CVE-2023-23520**	https://support.apple.com/en-us/HT213605 , https://support.apple.com/en-us/HT213606	O-APP-MACO-170323/1036
Exposure of Resource to Wrong Sphere	27-Feb-2023	5.5	The issue was addressed with improved memory handling This issue is fixed in macOS Ventura 13.2. An app may be able to disclose kernel memory.. **CVE ID : CVE-2023-23501**	https://support.apple.com/en-us/HT213605	O-APP-MACO-170323/1037
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences.	https://support.apple.com/en-us/HT213598 , https://support.apple.com/en-us/HT213605 , https://support.apple.com/en-us/HT213606	O-APP-MACO-170323/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23503	, https://support.apple.com/en-us/HT213601 , https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.2. An app may be able to access user-sensitive data. **CVE ID : CVE-2023-23506**	https://support.apple.com/en-us/HT213605	O-APP-MACO-170323/1039
N/A	27-Feb-2023	5.5	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.2. An app may be able to access a user's Safari history. **CVE ID : CVE-2023-23510**	https://support.apple.com/en-us/HT213605	O-APP-MACO-170323/1040
N/A	27-Feb-2023	5.5	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Ventura 13.2.1. An app may be able to observe unprotected user data.. **CVE ID : CVE-2023-23522**	https://support.apple.com/en-us/HT213633	O-APP-MACO-170323/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 13.2.1					
Access of Resource Using Incompatible Type ('Type Confusion')	27-Feb-2023	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, Safari 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2023-23529**	https://support.apple.com/en-us/HT213638, https://support.apple.com/en-us/HT213635, https://support.apple.com/en-us/HT213633	O-APP-MACO-170323/1042
Uncontrolled Resource Consumption	27-Feb-2023	7.5	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of-service. **CVE ID : CVE-2023-23524**	https://support.apple.com/en-us/HT213634, https://support.apple.com/en-us/HT213635, https://support.apple.com/en-us/HT213632, https://support.apple.com/en-us/HT213633	O-APP-MACO-170323/1043
Affected Version(s): From (including) 11.0 Up to (excluding) 11.7.3					
N/A	27-Feb-2023	7.8	A logic issue was addressed with	https://support.apple.com/	O-APP-MACO-170323/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to gain root privileges. **CVE ID : CVE-2023-23497**	en-us/HT213605, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604	
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access user-sensitive data. **CVE ID : CVE-2023-23499**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1045
N/A	27-Feb-2023	5.5	The issue was addressed with	https://support.apple.com/	O-APP-MACO-170323/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23508**	en-us/HT213605, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604	
Insertion of Sensitive Information into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. **CVE ID : CVE-2023-23505**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1047
Affected Version(s): From (including) 12.0 Up to (excluding) 12.6.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Feb-2023	9.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution. **CVE ID : CVE-2023-23513**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604	O-APP-MACO-170323/1048
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23517**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/	O-APP-MACO-170323/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213599	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23518**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1050
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.6.3					
N/A	27-Feb-2023	7.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to gain root privileges.	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213603, https://suppo	O-APP-MACO-170323/1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23497	rt.apple.com/en-us/HT213604	
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-23504**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1052
N/A	27-Feb-2023	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213604	O-APP-MACO-170323/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23507		
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access user-sensitive data. **CVE ID : CVE-2023-23499**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1054
N/A	27-Feb-2023	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/	O-APP-MACO-170323/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to determine kernel memory layout. **CVE ID : CVE-2023-23502**	en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23508**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604	O-APP-MACO-170323/1056
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23511**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/	O-APP-MACO-170323/1057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213601, https://support.apple.com/en-us/HT213599	
Improper Authentication	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3. An encrypted volume may be unmounted and remounted by a different user without prompting for the password. **CVE ID : CVE-2023-23493**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213604	O-APP-MACO-170323/1058
Insertion of Sensitive Information into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. **CVE ID : CVE-2023-23505**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603,	O-APP-MACO-170323/1059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213599	
Affected Version(s): From (including) 13.0 Up to (excluding) 13.2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Feb-2023	9.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution. **CVE ID : CVE-2023-23513**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604	O-APP-MACO-170323/1060
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/	O-APP-MACO-170323/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23517	en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23518**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1062
N/A	27-Feb-2023	7.8	A logic issue was addressed with	https://support.apple.com/	O-APP-MACO-170323/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to gain root privileges. **CVE ID : CVE-2023-23497**	en-us/HT213605, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604	
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-23504**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1064
N/A	27-Feb-2023	7.8	The issue was addressed with	https://support.apple.com/	O-APP-MACO-170323/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved bounds checks. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-23507**	en-us/HT213605, https://support.apple.com/en-us/HT213604	
N/A	27-Feb-2023	6.5	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Visiting a website may lead to an app denial-of-service. **CVE ID : CVE-2023-23512**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1066
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-	O-APP-MACO-170323/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access user-sensitive data. **CVE ID : CVE-2023-23499**	us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2023-23500**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1068
N/A	27-Feb-2023	5.5	An information disclosure issue was addressed by	https://support.apple.com/en-	O-APP-MACO-170323/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing the vulnerable code. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to determine kernel memory layout. **CVE ID : CVE-2023-23502**	us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, macOS Big Sur 11.7.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23508**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604	O-APP-MACO-170323/1070
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-	O-APP-MACO-170323/1071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23511**	us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
Improper Authentication	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3. An encrypted volume may be unmounted and remounted by a different user without prompting for the password. **CVE ID : CVE-2023-23493**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213604	O-APP-MACO-170323/1072
N/A	27-Feb-2023	3.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, iOS 16.3 and iPadOS 16.3. The quoted original message	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://suppo	O-APP-MACO-170323/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be selected from the wrong email when forwarding an email from an Exchange account. **CVE ID : CVE-2023-23498**	rt.apple.com/en-us/HT213606	
Insertion of Sensitive Information into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. **CVE ID : CVE-2023-23505**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213599	O-APP-MACO-170323/1074
Affected Version(s): From (including) 13.0 Up to (excluding) 13.2.1					
Use After Free	27-Feb-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura	https://support.apple.com/en-us/HT213635, https://suppo	O-APP-MACO-170323/1075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.2.1, iOS 16.3.1 and iPadOS 16.3.1. An app may be able to execute arbitrary code with kernel privileges.. **CVE ID : CVE-2023-23514**	rt.apple.com/en-us/HT213633	
Product: tvos					
Affected Version(s): * Up to (excluding) 16.3					
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23496**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599, https://support.apple.com/en-us/HT213600	O-APP-TVOS-170323/1076
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-	O-APP-TVOS-170323/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23517**	us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23518**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-	O-APP-TVOS-170323/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213601 , https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-23504**	https://support.apple.com/en-us/HT213598 , https://support.apple.com/en-us/HT213605 , https://support.apple.com/en-us/HT213606 , https://support.apple.com/en-us/HT213604 , https://support.apple.com/en-us/HT213601 , https://support.apple.com/en-us/HT213599	O-APP-TVOS-170323/1079
Out-of-bounds Write	27-Feb-2023	7.5	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3	https://support.apple.com/en-us/HT213605 , https://support.apple.com/en-	O-APP-TVOS-170323/1080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 16.3, watchOS 9.3. Processing an image may lead to a denial-of-service. **CVE ID : CVE-2023-23519**	us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	6.5	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Visiting a website may lead to an app denial-of-service. **CVE ID : CVE-2023-23512**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-TVOS-170323/1081
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-	O-APP-TVOS-170323/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access user-sensitive data. **CVE ID : CVE-2023-23499**	us/HT213603, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2023-23500**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-TVOS-170323/1083
N/A	27-Feb-2023	5.5	An information disclosure issue was addressed by	https://support.apple.com/en-	O-APP-TVOS-170323/1084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing the vulnerable code. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to determine kernel memory layout. **CVE ID : CVE-2023-23502**	us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23503**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/	O-APP-TVOS-170323/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23511**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-TVOS-170323/1086
Affected Version(s): * Up to (excluding) 16.3.2					
Uncontrolled Resource Consumption	27-Feb-2023	7.5	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of-service.	https://support.apple.com/en-us/HT213634, https://support.apple.com/en-us/HT213635, https://support.apple.com/en-us/HT213632, https://suppo	O-APP-TVOS-170323/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23524	rt.apple.com/en-us/HT213633	
Product: watchos					
Affected Version(s): * Up to (excluding) 9.3					
N/A	27-Feb-2023	8.8	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23496**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599, https://support.apple.com/en-us/HT213600	O-APP-WATC-170323/1088
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603	O-APP-WATC-170323/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2023-23517**	, https://support.apple.com/en-us/HT213604 , https://support.apple.com/en-us/HT213601 , https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, Safari 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2023-23518**	https://support.apple.com/en-us/HT213605 , https://support.apple.com/en-us/HT213606 , https://support.apple.com/en-us/HT213603 , https://support.apple.com/en-us/HT213604 , https://support.apple.com/en-us/HT213601 , https://support.apple.com/	O-APP-WATC-170323/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213599	
N/A	27-Feb-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2023-23504**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-WATC-170323/1091
Out-of-bounds Write	27-Feb-2023	7.5	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Processing an image	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/	O-APP-WATC-170323/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may lead to a denial-of-service. **CVE ID : CVE-2023-23519**	en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	6.5	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.2, tvOS 16.3, iOS 16.3 and iPadOS 16.3, watchOS 9.3. Visiting a website may lead to an app denial-of-service. **CVE ID : CVE-2023-23512**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-WATC-170323/1093
N/A	27-Feb-2023	5.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access user-sensitive data. **CVE ID : CVE-2023-23499**	https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/	O-APP-WATC-170323/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2023-23500**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-WATC-170323/1095
N/A	27-Feb-2023	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.2,	https://support.apple.com/en-us/HT213605, https://support.apple.com/	O-APP-WATC-170323/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to determine kernel memory layout. **CVE ID : CVE-2023-23502**	en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
N/A	27-Feb-2023	5.5	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 15.7.3 and iPadOS 15.7.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23503**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	O-APP-WATC-170323/1097
N/A	27-Feb-2023	5.5	The issue was addressed with	https://support.apple.com/	O-APP-WATC-170323/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved memory handling. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, tvOS 16.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-23511**	en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213604, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213599	
Insertion of Sensitive Information into Log File	27-Feb-2023	3.3	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.2, macOS Monterey 12.6.3, iOS 15.7.3 and iPadOS 15.7.3, watchOS 9.3, iOS 16.3 and iPadOS 16.3, macOS Big Sur 11.7.3. An app may be able to access information about a user's contacts. **CVE ID : CVE-2023-23505**	https://support.apple.com/en-us/HT213598, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213603, https://support.apple.com/	O-APP-WATC-170323/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en-us/HT213604, https://support.apple.com/en-us/HT213599	
Affected Version(s): * Up to (excluding) 9.3.1					
Uncontrolled Resource Consumption	27-Feb-2023	7.5	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.2.1, iOS 16.3.1 and iPadOS 16.3.1, tvOS 16.3.2, watchOS 9.3.1. Processing a maliciously crafted certificate may lead to a denial-of-service. **CVE ID : CVE-2023-23524**	https://support.apple.com/en-us/HT213634, https://support.apple.com/en-us/HT213635, https://support.apple.com/en-us/HT213632, https://support.apple.com/en-us/HT213633	O-APP-WATC-170323/1100
Vendor: Asus					
Product: asmb8-ikvm_firmware					
Affected Version(s): * Up to (including) 1.14.51					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Feb-2023	9.8	ASUS ASMB8 iKVM firmware through 1.14.51 allows remote attackers to execute arbitrary code by using SNMP to create extensions, as demonstrated by snmpset for NET-SNMP-EXTEND-MIB with /bin/sh for command execution.	N/A	O-ASU-ASMB-170323/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26602		
Vendor: Axis					
Product: 207w_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	6.1	** UNSUPPORTED WHEN ASSIGNED ** A Vulnerability was discovered in Axis 207W network camera. There is a reflected XSS vulnerability in the web administration portal, which allows an attacker to execute arbitrary JavaScript via URL. **CVE ID : CVE-2023-22984**	N/A	O-AXI-207W-170323/1102
Vendor: Cisco					
Product: fxos					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	O-CIS-FXOS-170323/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Affected Version(s): * Up to (excluding) 2.6.1					
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	O-CIS-FXOS-170323/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: nexus_93180yc-fx3s_firmware					
Affected Version(s): -					
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx	O-CIS-NEXU-170323/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**		
Product: nexus_93180yc-fx3_firmware					
Affected Version(s): -					
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx	O-CIS-NEXU-170323/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**		
Product: nx-os					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	O-CIS-NX-O-170323/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Affected Version(s): * Up to (excluding) 10.2\\(4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	O-CIS-NX-O-170323/1108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Affected Version(s): * Up to (excluding) 8.2\\(9\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	O-CIS-NX-O-170323/1109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**		
Affected Version(s): * Up to (excluding) 9.3\\(10\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	7.8	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user. **CVE ID : CVE-2023-20050**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u	O-CIS-NX-O-170323/1110
Affected Version(s): 15.2\\(1g\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(2e\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(2f\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20089		
Affected Version(s): 15.2\\(2g\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(2h\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(3e\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-	O-CIS-NX-O-170323/1116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be	dos-ySCNZOpX	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(3f\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(3g\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(4d\\)					
Missing Release of Memory after	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco	https://sec.cloudapps.cisco.com/security/center/content	O-CIS-NX-O-170323/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device	/CiscoSecurity Advisory/cisco-sa-aci-lldp-dos-ySCNZOpX	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(4e\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(4f\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(5c\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(5d\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 15.2\\(5e\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20089		
Affected Version(s): 16.0\\(1g\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Affected Version(s): 16.0\\(1j\\)					
Missing Release of Memory after Effective Lifetime	23-Feb-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, adjacent attacker to cause a memory leak, which could result in an unexpected reload of the device. This vulnerability is due to incorrect error checking when parsing ingress LLDP packets. An attacker could exploit this vulnerability by sending a steady stream of crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX	O-CIS-NX-O-170323/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LLDP packets to an affected device. A successful exploit could allow the attacker to cause a memory leak, which could result in a denial of service (DoS) condition when the device unexpectedly reloads. Note: This vulnerability cannot be exploited by transit traffic through the device. The crafted LLDP packet must be targeted to a directly connected interface, and the attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). In addition, the attack surface for this vulnerability can be reduced by disabling LLDP on interfaces where it is not required. **CVE ID : CVE-2023-20089**		
Product: ucs_6200_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-	O-CIS-UCS_-170323/1127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**	cmdinj-XXBZjtR	
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software	https://sec.cloudapps.cisco.com/security/center/content	O-CIS-UCS_-170323/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**	/CiscoSecurity Advisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	
Product: ucs_6248up_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	O-CIS-UCS_-170323/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	O-CIS-UCS_-170323/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: ucs_6296up_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	O-CIS-UCS_-170323/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	O-CIS-UCS_-170323/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: ucs_6300_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	O-CIS-UCS_-170323/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	O-CIS-UCS_-170323/1134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: ucs_6324_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	O-CIS-UCS_-170323/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	O-CIS-UCS_-170323/1136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Product: ucs_6332-16up_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	O-CIS-UCS_-170323/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-	O-CIS-UCS_-170323/1138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**	bkpsky-H8FCQgsA	
Product: ucs_6332_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	O-CIS-UCS_-170323/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20015		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	O-CIS-UCS_-170323/1140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and other credentials. **CVE ID : CVE-2023-20016**		
Product: ucs_64108_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	O-CIS-UCS_-170323/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	O-CIS-UCS_-170323/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx	O-CIS-UCS_-170323/1143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**		
Product: ucs_6454_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute unauthorized commands within	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	O-CIS-UCS_-170323/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	O-CIS-UCS_-170323/1145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by logging in to the console port on an affected device. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx	O-CIS-UCS_-170323/1146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**		
Product: ucs_6536_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Feb-2023	6.7	A vulnerability in the CLI of Cisco Firepower 4100 Series, Cisco Firepower 9300 Security Appliances, and Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects could allow an authenticated, local attacker to inject unauthorized commands. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR	O-CIS-UCS_-170323/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute unauthorized commands within the CLI. An attacker with Administrator privileges could also execute arbitrary commands on the underlying operating system of Cisco UCS 6400 and 6500 Series Fabric Interconnects with root-level privileges. **CVE ID : CVE-2023-20015**		
Use of Insufficiently Random Values	23-Feb-2023	6.5	A vulnerability in the backup configuration feature of Cisco UCS Manager Software and in the configuration export feature of Cisco FXOS Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files. This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA	O-CIS-UCS_-170323/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials. **CVE ID : CVE-2023-20016**		
Improper Authentication	23-Feb-2023	4.6	A vulnerability in the CLI console login authentication of Cisco Nexus 9300-FX3 Series Fabric Extender (FEX) when used in UCS Fabric Interconnect deployments could allow an unauthenticated attacker with physical access to bypass authentication. This vulnerability is due to the improper implementation of the password validation function. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx	O-CIS-UCS_-170323/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging in to the console port on an affected device. A successful exploit could allow the attacker to bypass authentication and execute a limited set of commands local to the FEX, which could cause a device reboot and denial of service (DoS) condition. **CVE ID : CVE-2023-20012**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
N/A	22-Feb-2023	8.8	The mono package before 6.8.0.105+dfsg-3.3 for Debian allows arbitrary code execution because the application/x-ms-dos-executable MIME type is associated with an un-sandboxed Mono CLR interpreter. **CVE ID : CVE-2023-26314**	N/A	O-DEB-DEBI-170323/1150
Allocation of Resources Without Limits or Throttling	23-Feb-2023	7.5	An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning	https://security.netapp.com/advisory/ntap-20230309-0006/	O-DEB-DEBI-170323/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that a server response can be compressed multiple times and potentially with differentalgorithms. The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors. **CVE ID : CVE-2023-23916**		
Untrusted Search Path	23-Feb-2023	4.2	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running	https://nodejs.org/en/blog/vulnerability/february-2023-security-releases/	O-DEB-DEBI-170323/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with elevated privileges. **CVE ID : CVE-2023-23920**		
Affected Version(s): 11.0					
N/A	28-Feb-2023	9.8	SPIP before 4.2.1 allows Remote Code Execution via form values in the public area because serialization is mishandled. The fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1. **CVE ID : CVE-2023-27372**	https://git.spip.net/spip/spip/commit/5aedf49b89415a4df3eb775eee3801a2b4b88266, https://git.spip.net/spip/spip/commit/96fbeb38711c6706e62457f2b732a652a04a409d	O-DEB-DEBI-170323/1153
Allocation of Resources Without Limits or Throttling	23-Feb-2023	7.5	An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning that a server response can be compressed multiple times and potentially with differentalgorithms. The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to	https://security.netapp.com/advisory/ntap-20230309-0006/	O-DEB-DEBI-170323/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors. **CVE ID : CVE-2023-23916**		
Uncontrolled Resource Consumption	21-Feb-2023	6.5	Libreswan 4.9 allows remote attackers to cause a denial of service (assert failure and daemon restart) via crafted TS payload with an incorrect selector length. **CVE ID : CVE-2023-23009**	https://github.com/libreswan/libreswan/issues/954	O-DEB-DEBI-170323/1155
Vendor: Dell					
Product: a2000_firmware					
Affected Version(s): 9.0.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-	O-DEL-A200-170323/1156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	multiple-security	
Affected Version(s): 9.1.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-A200-170323/1157
Affected Version(s): 9.2.0.0					
Uncontrolled	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000,	https://www.dell.com/supp	O-DEL-A200-170323/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	ort/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	
Affected Version(s): 9.2.1.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-A200-170323/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.3.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-A200-170323/1160
Affected Version(s): 9.4.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-A200-170323/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.5.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-A200-170323/1162
Product: a200_firmware					
Affected Version(s): 9.0.0.0					
Uncontrolled Resource	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600,	https://www.dell.com/support/kbdoc/en-	O-DEL-A200-170323/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	
Affected Version(s): 9.1.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-A200-170323/1164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.2.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-A200-170323/1165
Affected Version(s): 9.2.1.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-A200-170323/1166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.3.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-A200-170323/1167
Affected Version(s): 9.4.0.0					
Uncontrolled Resource	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810	https://www.dell.com/support/kbdoc/en-us/00020989	O-DEL-A200-170323/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	5/dell-emc-powerscale-onefs-security-updates-for-multiple-security	
Affected Version(s): 9.5.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-A200-170323/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23689		
Product: emc_powerscale_onefs					
Affected Version(s): From (including) 9.4.0.0 Up to (including) 9.4.0.11					
Incorrect Default Permissions	28-Feb-2023	7.1	Dell PowerScale OneFS 9.4.0.x contains an incorrect default permissions vulnerability. A local malicious user could potentially exploit this vulnerability to overwrite arbitrary files causing denial of service. **CVE ID : CVE-2023-25540**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-EMC_-170323/1170
Product: f800_firmware					
Affected Version(s): 9.0.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F800-170323/1171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23689		
Affected Version(s): 9.1.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F800-170323/1172
Affected Version(s): 9.2.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F800-170323/1173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.2.1.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F800-170323/1174
Affected Version(s): 9.3.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-	O-DEL-F800-170323/1175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	onefs-security-updates-for-multiple-security	
Affected Version(s): 9.4.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F800-170323/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23689		
Affected Version(s): 9.5.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F800-170323/1177
Product: f810_firmware					
Affected Version(s): 9.0.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F810-170323/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.1.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F810-170323/1179
Affected Version(s): 9.2.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-	O-DEL-F810-170323/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	powerscale-onefs-security-updates-for-multiple-security	
Affected Version(s): 9.2.1.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F810-170323/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23689		
Affected Version(s): 9.3.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F810-170323/1182
Affected Version(s): 9.4.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F810-170323/1183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.5.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-F810-170323/1184
Product: h400_firmware					
Affected Version(s): 9.0.0.0					
Uncontrolled Resource	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-	O-DEL-H400-170323/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	powerscale-onefs-security-updates-for-multiple-security	
Affected Version(s): 9.1.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H400-170323/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23689		
Affected Version(s): 9.2.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H400-170323/1187
Affected Version(s): 9.2.1.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H400-170323/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.3.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H400-170323/1189
Affected Version(s): 9.4.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-	O-DEL-H400-170323/1190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	onefs-security-updates-for-multiple-security	
Affected Version(s): 9.5.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H400-170323/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23689		
Product: h500_firmware					
Affected Version(s): 9.0.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H500-170323/1192
Affected Version(s): 9.1.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H500-170323/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.2.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H500-170323/1194
Affected Version(s): 9.2.1.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-	O-DEL-H500-170323/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	powerscale-onefs-security-updates-for-multiple-security	
Affected Version(s): 9.3.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H500-170323/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23689		
Affected Version(s): 9.4.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H500-170323/1197
Affected Version(s): 9.5.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H500-170323/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Product: h5600_firmware					
Affected Version(s): 9.0.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H560-170323/1199
Affected Version(s): 9.1.0.0					
Uncontrolled Resource	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-	O-DEL-H560-170323/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	powerscale-onefs-security-updates-for-multiple-security	
Affected Version(s): 9.2.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H560-170323/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23689		
Affected Version(s): 9.2.1.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H560-170323/1202
Affected Version(s): 9.3.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H560-170323/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.4.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H560-170323/1204
Affected Version(s): 9.5.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-	O-DEL-H560-170323/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	onefs-security-updates-for-multiple-security	
Product: h600_firmware					
Affected Version(s): 9.0.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H600-170323/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23689		
Affected Version(s): 9.1.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H600-170323/1207
Affected Version(s): 9.2.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H600-170323/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**		
Affected Version(s): 9.2.1.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H600-170323/1209
Affected Version(s): 9.3.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-	O-DEL-H600-170323/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	onefs-security-updates-for-multiple-security	
Affected Version(s): 9.4.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H600-170323/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23689		
Affected Version(s): 9.5.0.0					
Uncontrolled Resource Consumption	28-Feb-2023	7.5	Dell PowerScale nodes A200, A2000, H400, H500, H600, H5600, F800, F810 integrated hardware management software contains an uncontrolled resource consumption vulnerability. This may allow an unauthenticated network host to impair built-in hardware management functionality and trigger OneFS data protection mechanism causing a denial of service. **CVE ID : CVE-2023-23689**	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	O-DEL-H600-170323/1212
Vendor: Draytek					
Product: vigor2960_firmware					
Affected Version(s): 1.5.1.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Feb-2023	5.5	A vulnerability classified as problematic has been found in DrayTek Vigor 2960 1.5.1.4. Affected is the function sub_1DF14 of the file /cgi-bin/mainfunction.cgi. The manipulation of the argument option	N/A	O-DRA-VIGO-170323/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the input /../etc/password leads to path traversal. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. VDB-221742 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1009**		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 36					
Allocation of Resources Without Limits or Throttling	23-Feb-2023	7.5	An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP compression algorithms, meaning that a server response can be compressed multiple times and potentially with differentalgorithms. The number of acceptable "links" in this "decompression chain" wascapped, but the cap was implemented on a per-header basis allowing a maliciousserver to	https://security.netapp.com/advisory/ntap-20230309-0006/	O-FED-FEDO-170323/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insert a virtually unlimited number of compression steps simply byusing many headers. The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying to and returning out of memory errors. **CVE ID : CVE-2023-23916**		
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit-389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2023-1055**	https://bugzilla.redhat.com/show_bug.cgi?id=2173517#c0	O-FED-FEDO-170323/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 37					
Exposure of Resource to Wrong Sphere	20-Feb-2023	7.5	In Epiphany (aka GNOME Web) through 43.0, untrusted web content can trick users into exfiltrating passwords, because autofill occurs in sandboxed contexts. **CVE ID : CVE-2023-26081**	https://gitlab.gnome.org/GNOME/epiphany/-/merge_requests/1275	O-FED-FEDO-170323/1216
Double Free	28-Feb-2023	7.2	Sudo before 1.9.13p2 has a double free in the per-command chroot feature. **CVE ID : CVE-2023-27320**	N/A	O-FED-FEDO-170323/1217
Improper Certificate Validation	27-Feb-2023	5.5	A flaw was found in RHDS 11 and RHDS 12. While browsing entries LDAP tries to decode the userPassword attribute instead of the userCertificate attribute which could lead into sensitive information leaked. An attacker with a local account where the cockpit-389-ds is running can list the processes and display the hashed passwords. The highest threat from this vulnerability is to data confidentiality.	https://bugzilla.redhat.com/show_bug.cgi?id=2173517#c0	O-FED-FEDO-170323/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1055		
Vendor: Google					
Product: android					
Affected Version(s): -					
Use After Free	22-Feb-2023	8.8	Use after free in Web Payments API in Google Chrome on Android prior to 110.0.5481.177 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0927**	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	O-GOO-ANDR-170323/1219
Use After Free	28-Feb-2023	7.8	In several functions of the Android Linux kernel, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257443051References: Upstream kernel	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20937		
Use After Free	28-Feb-2023	7.8	In binder_transaction_buffer_release of binder.c, there is a possible use after free due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257685302References: Upstream kernel **CVE ID : CVE-2023-20938**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1221
Affected Version(s): 10.0					
Use After Free	28-Feb-2023	7.8	In several functions of MediaCodec.cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-245860753 **CVE ID : CVE-2023-20933**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.8	In clearApplicationUserData of ActivityManagerService.java, there is a possible way to remove system files due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240267890 **CVE ID : CVE-2023-20943**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1223
Deserialization of Untrusted Data	28-Feb-2023	7.8	In run of ChooseTypeAndAccountActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-244154558 **CVE ID : CVE-2023-20944**		
Out-of-bounds Write	28-Feb-2023	7.8	In phNciNfc_MfCreateXchgDataHdr of phNxpExtns_MifareStd.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-246932269 **CVE ID : CVE-2023-20945**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1225
Improper Input Validation	28-Feb-2023	3.3	In onCreatePreferences of EditInfoFragment.java, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-248251018 **CVE ID : CVE-2023-20932**		
Affected Version(s): 11.0					
N/A	28-Feb-2023	9.8	In onStart of BluetoothSwitchPreferenceController.java, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-244423101 **CVE ID : CVE-2023-20946**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1227
Use After Free	28-Feb-2023	7.8	In several functions of MediaCodec.cpp,	https://source.android.com	O-GOO-ANDR-170323/1228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-245860753 **CVE ID : CVE-2023-20933**	/security/bulletin/2023-02-01	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.8	In clearApplicationUserData of ActivityManagerService.java, there is a possible way to remove system files due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240267890	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20943		
Deserialization of Untrusted Data	28-Feb-2023	7.8	In run of ChooseTypeAndAccountActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-244154558 **CVE ID : CVE-2023-20944**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1230
Improper Input Validation	28-Feb-2023	3.3	In onCreatePreferences of EditInfoFragment.java, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-248251018 **CVE ID : CVE-2023-20932**		
Affected Version(s): 12.0					
N/A	28-Feb-2023	9.8	In onStart of BluetoothSwitchPreferenceController.java, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-244423101 **CVE ID : CVE-2023-20946**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1232
Use After Free	28-Feb-2023	7.8	In several functions of MediaCodec.cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-245860753 **CVE ID : CVE-2023-20933**		
N/A	28-Feb-2023	7.8	In resolveAttributionSource of ServiceUtilities.cpp, there is a possible way to disable the microphone privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-258672042 **CVE ID : CVE-2023-20934**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1234
Improper Locking	28-Feb-2023	7.8	In multiple functions of looper_backed_event_loop.cpp, there is a possible way to	https://source.android.com/security/bull	O-GOO-ANDR-170323/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			corrupt memory due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-243362981 **CVE ID : CVE-2023-20939**	etin/2023-02-01	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Feb-2023	7.8	In clearApplicationUserData of ActivityManagerService.java, there is a possible way to remove system files due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240267890 **CVE ID : CVE-2023-20943**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	28-Feb-2023	7.8	In run of ChooseTypeAndAccountActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-244154558 **CVE ID : CVE-2023-20944**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1237
Out-of-bounds Read	28-Feb-2023	7.5	In dropFramesUntilIframe of AAVCAssembler.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A-230630526 **CVE ID : CVE-2023-20948**		
Improper Input Validation	28-Feb-2023	3.3	In onCreatePreferences of EditInfoFragment.java, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-248251018 **CVE ID : CVE-2023-20932**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1239
Affected Version(s): 12.1					
N/A	28-Feb-2023	9.8	In onStart of BluetoothSwitchPreferenceController.java, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-244423101 **CVE ID : CVE-2023-20946**		
Use After Free	28-Feb-2023	7.8	In several functions of MediaCodec.cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-245860753 **CVE ID : CVE-2023-20933**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1241
N/A	28-Feb-2023	7.8	In resolveAttributionSource of ServiceUtilities.cpp, there is a possible way to disable the microphone privacy indicator due to a	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-258672042 **CVE ID : CVE-2023-20934**		
Improper Locking	28-Feb-2023	7.8	In multiple functions of looper_backed_event_loop.cpp, there is a possible way to corrupt memory due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-243362981 **CVE ID : CVE-2023-20939**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1243
Improper Limitation of a Pathname to a	28-Feb-2023	7.8	In clearApplicationUserData of ActivityManagerService.java, there is a	https://source.android.com/security/bull	O-GOO-ANDR-170323/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			possible way to remove system files due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240267890 **CVE ID : CVE-2023-20943**	etin/2023-02-01	
Deserialization of Untrusted Data	28-Feb-2023	7.8	In run of ChooseTypeAndAccountActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-244154558	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20944		
Out-of-bounds Read	28-Feb-2023	7.5	In dropFramesUntilIframe of AAVCAssembler.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-230630526 **CVE ID : CVE-2023-20948**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1246
Improper Input Validation	28-Feb-2023	3.3	In onCreatePreferences of EditInfoFragment.java, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-248251018 **CVE ID : CVE-2023-20932**		
Affected Version(s): 13.0					
N/A	28-Feb-2023	9.8	In onStart of BluetoothSwitchPreferenceController.java, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-244423101 **CVE ID : CVE-2023-20946**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1248
Use After Free	28-Feb-2023	7.8	In several functions of MediaCodec.cpp, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-245860753 **CVE ID : CVE-2023-20933**		
N/A	28-Feb-2023	7.8	In resolveAttributionSource of ServiceUtilities.cpp, there is a possible way to disable the microphone privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-258672042 **CVE ID : CVE-2023-20934**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1250
Improper Locking	28-Feb-2023	7.8	In multiple functions of looper_backed_event_loop.cpp, there is a possible way to corrupt memory due	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-243362981 **CVE ID : CVE-2023-20939**		
Improper Verification of Cryptographic Signature	28-Feb-2023	7.8	In the Android operating system, there is a possible way to replace a boot partition due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256237041 **CVE ID : CVE-2023-20940**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1252
Improper Limitation of a Pathname to a Restricted Directory	28-Feb-2023	7.8	In clearApplicationUserData of ActivityManagerService.java, there is a possible way to remove system files	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240267890 **CVE ID : CVE-2023-20943**		
Deserialization of Untrusted Data	28-Feb-2023	7.8	In run of ChooseTypeAndAccountActivity.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-244154558 **CVE ID : CVE-2023-20944**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	28-Feb-2023	7.5	In dropFramesUntilIframe of AAVCAssembler.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-230630526 **CVE ID : CVE-2023-20948**	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1255
Improper Input Validation	28-Feb-2023	3.3	In onCreatePreferences of EditInfoFragment.java, there is a possible way to read contacts belonging to other users due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-	https://source.android.com/security/bulletin/2023-02-01	O-GOO-ANDR-170323/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11 Android-12 Android-12L Android-13Android ID: A-248251018 **CVE ID : CVE-2023-20932**		
Vendor: H3C					
Product: a210-g_firmware					
Affected Version(s): a210-gv100r005					
Improper Authentication	22-Feb-2023	9.8	An access control issue in H3C A210-G A210-GV100R005 allows attackers to authenticate without a password. **CVE ID : CVE-2023-24093**	N/A	O-H3C-A210-170323/1257
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Feb-2023	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 246333 **CVE ID : CVE-2023-24960**	https://www.ibm.com/support/pages/node/6953521, https://exchange.xforce.ibmcloud.com/vulnerabilities/246333	O-IBM-AIX-170323/1258
Cleartext Storage of Sensitive	17-Feb-2023	5.5	IBM InfoSphere Information Server 11.7 could allow a local user to obtain	https://exchange.xforce.ibmcloud.com/vulnerabilities/2	O-IBM-AIX-170323/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			sensitive information from a log files. IBM X-Force ID: 246463. **CVE ID : CVE-2023-24964**	46463, https://www.ibm.com/support/pages/node/6953519	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247646. **CVE ID : CVE-2023-25928**	https://exchange.xforce.ibmcloud.com/vulnerabilities/247646, https://www.ibm.com/support/pages/node/6956598	O-IBM-AIX-170323/1260
Vendor: Korenix					
Product: jetwave_2111l_firmware					
Affected Version(s): * Up to (excluding) 1.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1261
Improper Neutralization of	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series	N/A	O-KOR-JETW-170323/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**		
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1263
Product: jetwave_2111_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1264
Improper Neutralization of Special Elements used in a	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via	N/A	O-KOR-JETW-170323/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			/goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**		
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1266
Product: jetwave_2114_firmware					
Affected Version(s): * Up to (excluding) 1.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1267
Improper Neutralization of Special Elements used in a Command ('Comman	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd	N/A	O-KOR-JETW-170323/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**		
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1269
Product: jetwave_2211c_firmware					
Affected Version(s): * Up to (excluding) 1.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1270
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root.	N/A	O-KOR-JETW-170323/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23295		
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1272
Product: jetwave_2212g_firmware					
Affected Version(s): 1.3.t					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1273
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1275
Product: jetwave_2212s_firmware					
Affected Version(s): 1.3.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1276
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1277
Uncontrolled Resource	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series	N/A	O-KOR-JETW-170323/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**		
Product: jetwave_2212x_firmware					
Affected Version(s): 1.3.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1279
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1280
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via	N/A	O-KOR-JETW-170323/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/formDefault. **CVE ID : CVE-2023-23296**		
Product: jetwave_2411l_firmware					
Affected Version(s): * Up to (excluding) 1.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1282
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1283
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault.	N/A	O-KOR-JETW-170323/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23296		
Product: jetwave_2411_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1285
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1286
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1287
Product: jetwave_2414_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1288
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1289
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1290
Product: jetwave_2424_firmware					
Affected Version(s): * Up to (excluding) 1.3					
Improper Neutralizat	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and	N/A	O-KOR-JETW-170323/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1292
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1293
Product: jetwave_2460_firmware					
Affected Version(s): * Up to (excluding) 1.6					
Improper Neutralization of Special Elements	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command	N/A	O-KOR-JETW-170323/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1295
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1296
Product: jetwave_3220_v3_firmware					
Affected Version(s): * Up to (excluding) 1.7					
Improper Neutralization of Special Elements used in a Command ('Comman	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter	N/A	O-KOR-JETW-170323/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			to execute commands as root. **CVE ID : CVE-2023-23294**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1298
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1299
Product: jetwave_3420_v3_firmware					
Affected Version(s): * Up to (excluding) 1.7					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root.	N/A	O-KOR-JETW-170323/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23294		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1301
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1302
Product: jetwave_4221hp-e_firmware					
Affected Version(s): * Up to (including) 1.3.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix JetWave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection. An attacker can modify the file_name parameter to execute commands as root. **CVE ID : CVE-2023-23294**	N/A	O-KOR-JETW-170323/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Feb-2023	8.8	Korenix Jetwave 4200 Series 1.3.0 and JetWave 3000 Series 1.6.0 are vulnerable to Command Injection via /goform/formSysCmd. An attacker an modify the sysCmd parameter in order to execute commands as root. **CVE ID : CVE-2023-23295**	N/A	O-KOR-JETW-170323/1304
Uncontrolled Resource Consumption	23-Feb-2023	6.5	Korenix JetWave 4200 Series 1.3.0 and JetWave 3200 Series 1.6.0 are vulnerable to Denial of Service via /goform/formDefault. **CVE ID : CVE-2023-23296**	N/A	O-KOR-JETW-170323/1305
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Feb-2023	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 246333	https://www.ibm.com/support/pages/node/6953521, https://exchange.xforce.ibmcloud.com/vulnerabilities/246333	O-LIN-LINU-170323/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24960		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26. **CVE ID : CVE-2023-26020**	https://docs.craftercms.org/en/4.0/security/advisory.html#cv-2023021701	O-LIN-LINU-170323/1307
Cleartext Storage of Sensitive Information	17-Feb-2023	5.5	IBM InfoSphere Information Server 11.7 could allow a local user to obtain sensitive information from a log files. IBM X-Force ID: 246463. **CVE ID : CVE-2023-24964**	https://exchange.xforce.ibmcloud.com/vulnerabilities/246463, https://www.ibm.com/support/pages/node/6953519	O-LIN-LINU-170323/1308
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	5.4	IBM Aspera Faspex 4.4.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials	https://www.ibm.com/support/pages/node/6952319, https://exchange.xforce.ibmcloud.com/vulnerabilities/244117	O-LIN-LINU-170323/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure within a trusted session. IBM X-Force ID: 244117. **CVE ID : CVE-2023-22868**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247646. **CVE ID : CVE-2023-25928**	https://exchange.xforce.ibmcloud.com/vulnerabilities/247646, https://www.ibm.com/support/pages/node/6956598	O-LIN-LINU-170323/1310
Affected Version(s): * Up to (excluding) 5.16.3					
NULL Pointer Dereference	28-Feb-2023	5.5	In the Linux kernel before 5.16.3, drivers/usb/dwc3/dwc3-qcom.c misinterprets the dwc3_qcom_create_urs_usb_platdev return value (expects it to be NULL in the error case, whereas it is actually an error pointer). **CVE ID : CVE-2023-22999**	https://github.com/torvalds/linux/commit/b52fe2dbb3e655eb1483000adfab68a219549e13	O-LIN-LINU-170323/1311
Affected Version(s): * Up to (excluding) 5.17					
N/A	28-Feb-2023	7.8	In the Linux kernel before 5.17, an error	https://github.com/torvalds	O-LIN-LINU-170323/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			path in dwc3_qcom_acpi_register_core in drivers/usb/dwc3/dwc3-qcom.c lacks certain platform_device_put and kfree calls. **CVE ID : CVE-2023-22995**	/linux/commit/fa0ef93868a6062babe1144df2807a8b1d4924d2	
Affected Version(s): * Up to (excluding) 5.17.2					
Missing Release of Resource after Effective Lifetime	28-Feb-2023	5.5	In the Linux kernel before 5.17.2, drivers/soc/qcom/qcom_aoss.c does not release an of_find_device_by_node reference after use, e.g., with put_device. **CVE ID : CVE-2023-22996**	https://github.com/torvalds/linux/commit/4b41a9d0fe3db5f91078a380f62f0572c3ecf2dd	O-LIN-LINU-170323/1313
Affected Version(s): * Up to (excluding) 6.0					
NULL Pointer Dereference	28-Feb-2023	5.5	In nf_tables_updtable, if nf_tables_table_enable returns an error, nft_trans_destroy is called to free the transaction object. nft_trans_destroy() calls list_del(), but the transaction was never placed on a list -- the list head is all zeroes, this results in a NULL pointer dereference. **CVE ID : CVE-2023-1095**	https://github.com/torvalds/linux/commit/580077855a40741cf511766129702d97ff02f4d9, https://bugzilla.redhat.com/show_bug.cgi?id=2173973	O-LIN-LINU-170323/1314
Affected Version(s): * Up to (excluding) 6.0.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Interpretation Conflict	28-Feb-2023	5.5	In the Linux kernel before 6.0.3, drivers/gpu/drm/virtio/virtgpu_object.c misinterprets the drm_gem_shmem_get_sg_table return value (expects it to be NULL in the error case, whereas it is actually an error pointer). **CVE ID : CVE-2023-22998**	https://github.com/torvalds/linux/commit/c24968734abfed81c8f93dc5f44a7b7a9aecadfa	O-LIN-LINU-170323/1315
Affected Version(s): * Up to (excluding) 6.1.13					
Double Free	25-Feb-2023	7.8	In the Linux kernel before 6.1.13, there is a double free in net/mpls/af_mpls.c upon an allocation failure (for registering the sysctl table under a new location) during the renaming of a device. **CVE ID : CVE-2023-26545**	https://github.com/torvalds/linux/commit/fda6c89fe3d9aca073495a664e1d5aea28cd4377	O-LIN-LINU-170323/1316
Affected Version(s): * Up to (excluding) 6.1.2					
NULL Pointer Dereference	28-Feb-2023	5.5	In the Linux kernel before 6.1.2, kernel/module/decompress.c misinterprets the module_get_next_page return value (expects it to be NULL in the error case, whereas it is actually an error pointer).	https://github.com/torvalds/linux/commit/45af1d7aae7d5520d2858f8517a1342646f015db	O-LIN-LINU-170323/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22997		
Affected Version(s): * Up to (excluding) 6.2					
Use After Free	28-Feb-2023	7.8	There is a use-after-free vulnerability in the Linux Kernel which can be exploited to achieve local privilege escalation. To reach the vulnerability kernel configuration flag CONFIG_TLS or CONFIG_XFRM_ESPINTCP has to be configured, but the operation does not require any privilege. There is a use-after-free bug of icsk_ulp_data of a struct inet_connection_sock. When CONFIG_TLS is enabled, user can install a tls context (struct tls_context) on a connected tcp socket. The context is not cleared if this socket is disconnected and reused as a listener. If a new socket is created from the listener, the context is inherited and vulnerable. The setsockopt TCP_ULP operation does not require any privilege. We recommend	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=2c02d41d71f90a5168391b6a5f2954112ba2307c, https://kernel.dance/#2c02d41d71f90a5168391b6a5f2954112ba2307c	O-LIN-LINU-170323/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrading past commit 2c02d41d71f90a5168391b6a5f2954112ba2307c **CVE ID : CVE-2023-0461**		
Affected Version(s): * Up to (excluding) 6.2.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Feb-2023	5.7	An issue was discovered in the Linux kernel through 6.2.0-rc2. drivers/tty/vcc.c has a race condition and resultant use-after-free if a physically proximate attacker removes a VCC device while calling open(), aka a race condition between vcc_open() and vcc_remove(). **CVE ID : CVE-2023-23039**	https://lkml.org/lkml/2023/1/1/169	O-LIN-LINU-170323/1319
Affected Version(s): * Up to (including) 6.1.12					
Integer Overflow or Wraparound	21-Feb-2023	7.8	afu_mmio_region_get_by_offset in drivers/fpga/dfl-afu-region.c in the Linux kernel through 6.1.12 has an integer overflow. **CVE ID : CVE-2023-26242**	https://patchwork.kernel.org/project/linux-fpga/patch/202302060543 26.89323-1-k1rh4.lee@gmail.com	O-LIN-LINU-170323/1320
Affected Version(s): 6.0.8					
Use After Free	25-Feb-2023	7.8	In the Linux kernel 6.0.8, there is a use-after-free in run_unpack in fs/ntfs3/run.c,	N/A	O-LIN-LINU-170323/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			related to a difference between NTFS sector size and media sector size. **CVE ID : CVE-2023-26544**		
Use After Free	26-Feb-2023	7.8	In the Linux kernel 6.0.8, there is a use-after-free in inode_cgwb_move_to_attached in fs/fs-writeback.c, related to __list_del_entry_valid. **CVE ID : CVE-2023-26605**	N/A	O-LIN-LINU-170323/1322
Use After Free	26-Feb-2023	7.8	In the Linux kernel 6.0.8, there is a use-after-free in ntfs_trim_fs in fs/ntfs3/bitmap.c. **CVE ID : CVE-2023-26606**	N/A	O-LIN-LINU-170323/1323
Out-of-bounds Read	26-Feb-2023	7.1	In the Linux kernel 6.0.8, there is an out-of-bounds read in ntfs_attr_find in fs/ntfs/attrib.c. **CVE ID : CVE-2023-26607**	N/A	O-LIN-LINU-170323/1324
Affected Version(s): 6.2					
Use After Free	28-Feb-2023	7.8	There is a use-after-free vulnerability in the Linux Kernel which can be exploited to achieve local privilege escalation. To reach the vulnerability kernel configuration flag CONFIG_TLS or	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=2c02d41d71f90a5168391b6a5f2954112ba2307c,	O-LIN-LINU-170323/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CONFIG_XFRM_ESPINTCP has to be configured, but the operation does not require any privilege. There is a use-after-free bug of icsk_ulp_data of a struct inet_connection_sock. When CONFIG_TLS is enabled, user can install a tls context (struct tls_context) on a connected tcp socket. The context is not cleared if this socket is disconnected and reused as a listener. If a new socket is created from the listener, the context is inherited and vulnerable. The setsockopt TCP_ULP operation does not require any privilege. We recommend upgrading past commit 2c02d41d71f90a5168391b6a5f2954112ba2307c **CVE ID : CVE-2023-0461**	https://kernel.dance/#2c02d41d71f90a5168391b6a5f2954112ba2307c	
Missing Release of Memory after Effective Lifetime	23-Feb-2023	5.5	A flaw possibility of memory leak in the Linux kernel cpu_entry_area mapping of X86 CPU data to memory was	https://git.kernel.org/linus/97e3d26b5e5f371b3ee223d94dd123e6c442ba80	O-LIN-LINU-170323/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			found in the way user can guess location of exception stack(s) or other important data. A local user could use this flaw to get access to some important data with expected location in memory. **CVE ID : CVE-2023-0597**		
Affected Version(s): 6.2.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Feb-2023	5.7	An issue was discovered in the Linux kernel through 6.2.0-rc2. drivers/tty/vcc.c has a race condition and resultant use-after-free if a physically proximate attacker removes a VCC device while calling open(), aka a race condition between vcc_open() and vcc_remove(). **CVE ID : CVE-2023-23039**	https://lkml.org/lkml/2023/1/1/169	O-LIN-LINU-170323/1327
Affected Version(s): From (including) 5.6 Up to (excluding) 5.10.161					
Use After Free	17-Feb-2023	5.5	Due to a vulnerability in the io_uring subsystem, it is possible to leak kernel memory information to the user process. timens_install calls current_is_single_threaded to determine if	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/io_uring?h=linux-5.10.y&id=788d0824269bef539fe31a785	O-LIN-LINU-170323/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the current process is single-threaded, but this call does not consider io_uring's io_worker threads, thus it is possible to insert a time namespace's vvar page to process's memory space via a page fault. When this time namespace is destroyed, the vvar page is also freed, but not removed from the process' memory, and a next page allocated by the kernel will be still available from the user-space process and can leak memory contents via this (read-only) use-after-free vulnerability. We recommend upgrading past version 5.10.161 or commit 788d0824269bef539fe31a785b1517882eafed93 https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/io_uring **CVE ID : CVE-2023-23586**	b1517882eafed93, https://kernel.dance/#788d0824269bef539fe31a785b1517882eafed93	
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	17-Feb-2023	8.8	Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Kron Tech Single Connect on Windows allows Privilege Abuse. This issue affects Single Connect: 2.16. **CVE ID : CVE-2023-0882**	https://docs.krontech.com/singleconnect-2-16/update-patch-rdp-proxy-idor-vulnerability	O-MIC-WIND-170323/1329
Use After Free	22-Feb-2023	8.8	Use after free in WebRTC in Google Chrome on Windows prior to 110.0.5481.177 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-0932**	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	O-MIC-WIND-170323/1330
Improper Control of Generation of Code ('Code Injection')	24-Feb-2023	7.8	A vulnerability has been found in MarkText up to 0.17.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the component WSH JScript Handler. The manipulation leads to code injection. Local access is	N/A	O-MIC-WIND-170323/1331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-221737 was assigned to this vulnerability. **CVE ID : CVE-2023-1004**		
Improper Initialization	26-Feb-2023	7.8	A vulnerability, which was classified as critical, has been found in TechPowerUp Ryzen DRAM Calculator 1.2.0.5. This issue affects some unknown processing in the library WinRing0x64.sys. The manipulation leads to improper initialization. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-221807. **CVE ID : CVE-2023-1048**	N/A	O-MIC-WIND-170323/1332
Out-of-bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	O-MIC-WIND-170323/1333

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-2023-22237**		
Improper Input Validation	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an Improper Input Validation 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-2023-21574**	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	O-MIC-WIND-170323/1334
Out-of-bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (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	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	O-MIC-WIND-170323/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-21575**		
Out-of-bounds Write	17-Feb-2023	7.8	Photoshop version 23.5.3 (and earlier), 24.1 (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-2023-21576**	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	O-MIC-WIND-170323/1336
Out-of-bounds Write	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (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-2023-22238**	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	O-MIC-WIND-170323/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Feb-2023	7.8	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an Improper Input Validation 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-2023-22239**	https://helpx.adobe.com/security/products/after_effects/apsb23-02.html	O-MIC-WIND-170323/1338
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (and earlier) are affected by a Stack-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-2023-22243**	https://helpx.adobe.com/security/products/animate/apsb23-15.html	O-MIC-WIND-170323/1339
Use After Free	17-Feb-2023	7.8	Adobe Premiere Rush version 2.6 (and earlier) is affected by a Use	https://helpx.adobe.com/security/products/premiere_r	O-MIC-WIND-170323/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-22244**	ush/apsb23-14.html	
Use After Free	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (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-2023-22246**	https://helpx.adobe.com/security/products/animate/apsb23-15.html	O-MIC-WIND-170323/1341
Out-of-bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (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/framemaker/apsb23-06.html	O-MIC-WIND-170323/1342

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-2023-21619**		
Improper Privilege Management	16-Feb-2023	7.8	A vulnerability has been identified that, if exploited, could result in a local user elevating their privilege level to NT AUTHORITY\SYSTEM on a Citrix Virtual Apps and Desktops Windows VDA. **CVE ID : CVE-2023-24483**	https://support.citrix.com/article/CTX477616/citrix-virtual-apps-and-desktops-security-bulletin-for-cve202324483	O-MIC-WIND-170323/1343
Improper Input Validation	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and earlier) are affected by an Improper Input Validation 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-2023-21621**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	O-MIC-WIND-170323/1344
Out-of-bounds Write	17-Feb-2023	7.8	FrameMaker 2020 Update 4 (and earlier), 2022 (and	https://helpx.adobe.com/security/produc	O-MIC-WIND-170323/1345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-21622**	ts/framemaker/apsb23-06.html	
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by a Stack-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-2023-22226**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-MIC-WIND-170323/1346
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-MIC-WIND-170323/1347

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-2023-22227**		
Improper Input Validation	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an Improper Input Validation 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-2023-22228**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-MIC-WIND-170323/1348
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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.	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-MIC-WIND-170323/1349

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-2023-22229**		
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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-2023-22230**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-MIC-WIND-170323/1350
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Premiere Rush version 2.6 (and earlier) is affected by a Stack-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/premiere_rush/apsb23-14.html	O-MIC-WIND-170323/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-22234**		
Out-of-bounds Write	17-Feb-2023	7.8	Adobe Animate versions 22.0.8 (and earlier) and 23.0.0 (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-2023-22236**	https://helpx.adobe.com/security/products/animate/apsb23-15.html	O-MIC-WIND-170323/1352
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Feb-2023	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 246333 **CVE ID : CVE-2023-24960**	https://www.ibm.com/support/pages/node/6953521, https://exchange.xforce.ibmcloud.com/vulnerabilities/246333	O-MIC-WIND-170323/1353
Improper Neutralizat	22-Feb-2023	7.2	VMware Carbon Black App Control	https://www.vmware.com/	O-MIC-WIND-170323/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements in Output Used by a Downstream Component ('Injection')			8.7.x prior to 8.7.8, 8.8.x prior to 8.8.6, and 8.9.x.prior to 8.9.4 contain an injection vulnerability. A malicious actor with privileged access to the App Control administration console may be able to use specially crafted input allowing access to the underlying server operating system. **CVE ID : CVE-2023-20858**	security/advisories/VMSA-2023-0004.html	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Feb-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crafter Studio on Linux, MacOS, Windows, x86, ARM, 64 bit allows SQL Injection.This issue affects CrafterCMS v4.0 from 4.0.0 through 4.0.1, and v3.1 from 3.1.0 through 3.1.26. **CVE ID : CVE-2023-26020**	https://docs.craftercms.org/en/4.0/security/advisory.html#cv-2023021701	O-MIC-WIND-170323/1355
Out-of-bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (and earlier) are affected by an out-of-bounds read	https://helpx.adobe.com/security/products/photoshop	O-MIC-WIND-170323/1356

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-2023-21577**	/apsb23-11.html	
Out-of-bounds Read	17-Feb-2023	5.5	Photoshop version 23.5.3 (and earlier), 24.1 (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-2023-21578**	https://helpx.adobe.com/security/products/photoshop/apsb23-11.html	O-MIC-WIND-170323/1357
Out-of-bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (and earlier) are affected by an out-of-bounds read	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-MIC-WIND-170323/1358

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-2023-21583**		
Use After Free	17-Feb-2023	5.5	FrameMaker 2020 Update 4 (and earlier), 2022 (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-2023-21584**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	O-MIC-WIND-170323/1359
NULL Pointer Dereference	17-Feb-2023	5.5	Adobe InDesign versions ID18.1 (and earlier) and ID17.4 (and earlier) are affected by a NULL Pointer Dereference	https://helpx.adobe.com/security/products/indesign/a	O-MIC-WIND-170323/1360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service 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-2023-21593**	psb23-12.html	
Out-of-bounds Read	17-Feb-2023	5.5	FrameMaker 2020 Update 4 (and earlier), 2022 (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-2023-21620**	https://helpx.adobe.com/security/products/framemaker/apsb23-06.html	O-MIC-WIND-170323/1361
Out-of-bounds Read	17-Feb-2023	5.5	After Affects versions 23.1 (and earlier), 22.6.3 (and earlier) are affected by an out-of-bounds read vulnerability	https://helpx.adobe.com/security/products/after_effect	O-MIC-WIND-170323/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-22233**	s/apsb23-02.html	
Out-of-bounds Read	17-Feb-2023	5.5	Adobe Bridge versions 12.0.3 (and earlier) and 13.0.1 (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-2023-22231**	https://helpx.adobe.com/security/products/bridge/apsb23-09.html	O-MIC-WIND-170323/1363
Cleartext Storage of Sensitive Information	17-Feb-2023	5.5	IBM InfoSphere Information Server 11.7 could allow a local user to obtain sensitive information	https://exchange.xforce.ibmcloud.com/vulnerabilities/246463, https://www.i	O-MIC-WIND-170323/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from a log files. IBM X-Force ID: 246463. **CVE ID : CVE-2023-24964**	bm.com/support/pages/node/6953519	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Feb-2023	5.4	IBM Aspera Faspex 4.4.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244117. **CVE ID : CVE-2023-22868**	https://www.ibm.com/support/pages/node/6952319, https://exchange.xforce.ibmcloud.com/vulnerabilities/244117	O-MIC-WIND-170323/1365
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Feb-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 247646. **CVE ID : CVE-2023-25928**	https://exchange.xforce.ibmcloud.com/vulnerabilities/247646, https://www.ibm.com/support/pages/node/6956598	O-MIC-WIND-170323/1366
Vendor: Redhat					
Product: enterprise_linux					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 8.0					
NULL Pointer Dereference	28-Feb-2023	5.5	In nf_tables_updtable, if nf_tables_table_enable returns an error, nft_trans_destroy is called to free the transaction object. nft_trans_destroy() calls list_del(), but the transaction was never placed on a list -- the list head is all zeroes, this results in a NULL pointer dereference. **CVE ID : CVE-2023-1095**	https://github.com/torvalds/linux/commit/580077855a40741cf511766129702d97ff02f4d9, https://bugzilla.redhat.com/show_bug.cgi?id=2173973	O-RED-ENTE-170323/1367
Affected Version(s): 9.0					
NULL Pointer Dereference	28-Feb-2023	5.5	In nf_tables_updtable, if nf_tables_table_enable returns an error, nft_trans_destroy is called to free the transaction object. nft_trans_destroy() calls list_del(), but the transaction was never placed on a list -- the list head is all zeroes, this results in a NULL pointer dereference. **CVE ID : CVE-2023-1095**	https://github.com/torvalds/linux/commit/580077855a40741cf511766129702d97ff02f4d9, https://bugzilla.redhat.com/show_bug.cgi?id=2173973	O-RED-ENTE-170323/1368
Vendor: sick					
Product: fx0-gent00000_firmware					
Affected Version(s): 3.04					
Missing Authentica	20-Feb-2023	9.8	Missing Authentication for	https://sick.com/psirt	O-SIC-FX0--170323/1369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion for Critical Function			Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. **CVE ID : CVE-2023-23453**		
Affected Version(s): 3.05					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. **CVE ID : CVE-2023-23453**	https://sick.com/psirt	O-SIC-FX0--170323/1370
Product: fx0-gent00010_firmware					
Affected Version(s): 3.04					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an	https://sick.com/psirt	O-SIC-FX0--170323/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. **CVE ID : CVE-2023-23453**		
Affected Version(s): 3.05					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GENT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. **CVE ID : CVE-2023-23453**	https://sick.com/psirt	O-SIC-FX0--170323/1372
Product: fx0-gpnt00000_firmware					
Affected Version(s): 3.04					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted	https://sick.com/psirt	O-SIC-FX0--170323/1373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RK512 commands to the listener on TCP port 9000. **CVE ID : CVE-2023-23452**		
Affected Version(s): 3.05					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. **CVE ID : CVE-2023-23452**	https://sick.com/psirt	O-SIC-FX0--170323/1374
Product: fx0-gpnt00010_firmware					
Affected Version(s): 3.04					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000.	https://sick.com/psirt	O-SIC-FX0--170323/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23452		
Affected Version(s): 3.05					
Missing Authentication for Critical Function	20-Feb-2023	9.8	Missing Authentication for Critical Function in SICK FX0-GPNT v3 Firmware Version V3.04 and V3.05 allows an unprivileged remote attacker to achieve arbitrary remote code execution via maliciously crafted RK512 commands to the listener on TCP port 9000. **CVE ID : CVE-2023-23452**	https://sick.com/psirt	O-SIC-FX0--170323/1376
Vendor: Tenda					
Product: ac500_firmware					
Affected Version(s): 2.0.1.9\\(1307\\)					
Out-of-bounds Write	27-Feb-2023	9.8	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromRouteStatic via parameters entrys and mitInterface. **CVE ID : CVE-2023-25233**	N/A	O-TEN-AC50-170323/1377
Out-of-bounds Write	27-Feb-2023	9.8	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromAddressNat via parameters entrys and mitInterface.	N/A	O-TEN-AC50-170323/1378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25234		
Out-of-bounds Write	27-Feb-2023	7.5	Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function formOneSsidCfgSet via parameter ssid. **CVE ID : CVE-2023-25235**	https://github.com/Fuzzy33/Vluninfo_Repo/tree/main/CNVDs/113_2	O-TEN-AC50-170323/1379
Product: ax3_firmware					
Affected Version(s): 16.03.12.11					
Out-of-bounds Write	23-Feb-2023	9.8	Tenda AX3 V16.03.12.11 was discovered to contain a stack overflow via the timeType function at /goform/SetSysTimeCfg. **CVE ID : CVE-2023-24212**	N/A	O-TEN-AX3_-170323/1380
Product: cp3_firmware					
Affected Version(s): * Up to (including) 20220906024_2025					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.2211041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS	N/A	O-TEN-CP3_-170323/1381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tenda IT7-PRS<=V2209020908. **CVE ID : CVE-2023-23080**		
Product: cp7_firmware					
Affected Version(s): * Up to (including) 1.10.00.2211041403					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.2211041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7-PRS<=V2209020908. **CVE ID : CVE-2023-23080**	N/A	O-TEN-CP7_-170323/1382
Product: it7-lcs_firmware					
Affected Version(s): * Up to (including) 2209020914					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.2211041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-	N/A	O-TEN-IT7--170323/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7-PRS<=V2209020908. **CVE ID : CVE-2023-23080**		
Product: it7-pcs_firmware					
Affected Version(s): * Up to (including) 2209020914					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.2211041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7-PRS<=V2209020908. **CVE ID : CVE-2023-23080**	N/A	O-TEN-IT7--170323/1384
Product: it7-prs_firmware					
Affected Version(s): * Up to (including) 2209020908					
Improper Neutralization of Special Elements used in a Command	27-Feb-2023	9.8	Certain Tenda products are vulnerable to command injection. This affects Tenda CP7 Tenda CP7<=V11.10.00.221	N/A	O-TEN-IT7--170323/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			1041403 and Tenda CP3 v.10 Tenda CP3 v.10<=V20220906024_2025 and Tenda IT7-PCS Tenda IT7-PCS<=V2209020914 and Tenda IT7-LCS Tenda IT7-LCS<=V2209020914 and Tenda IT7-PRS Tenda IT7-PRS<=V2209020908. **CVE ID : CVE-2023-23080**		
Product: w30e_firmware					
Affected Version(s): v1.0.1.25\\(633\\)					
Out-of-bounds Write	27-Feb-2023	9.8	Tenda Router W30E V1.0.1.25(633) is vulnerable to Buffer Overflow in function fromRouteStatic via parameters entrys and mitInterface. **CVE ID : CVE-2023-25231**	N/A	O-TEN-W30E-170323/1386
Vendor: totolink					
Product: a7100ru_firmware					
Affected Version(s): 7.4cu.2313_b20191024					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Feb-2023	9.8	TOTOLink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability. **CVE ID : CVE-2023-24184**	N/A	O-TOT-A710-170323/1387
Improper Neutralization of	16-Feb-2023	9.8	TOTOlink A7100RU(V7.4cu.2313_B20191024) was	N/A	O-TOT-A710-170323/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			discovered to contain a command injection vulnerability via the province parameter at setting/delStaticDhcpRules. **CVE ID : CVE-2023-24236**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Feb-2023	9.8	TOTOlink A7100RU(V7.4cu.2313_B20191024) was discovered to contain a command injection vulnerability via the city parameter at setting/delStaticDhcpRules. **CVE ID : CVE-2023-24238**	N/A	O-TOT-A710-170323/1389
Product: a720r_firmware					
Affected Version(s): 4.1.5cu.532_b20210610					
Incorrect Authorization	17-Feb-2023	9.8	TOTOLINK A720R V4.1.5cu.532_B20210610 is vulnerable to Incorrect Access Control. **CVE ID : CVE-2023-23064**	N/A	O-TOT-A720-170323/1390
Vendor: Tp-link					
Product: archer_c50					
Affected Version(s): v2_160801					
Improper Resource Shutdown or Release	21-Feb-2023	6.5	A vulnerability was found in TP-Link Archer C50 V2_160801. It has been rated as	N/A	O-TP--ARCH-170323/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problematic. Affected by this issue is some unknown functionality of the component Web Management Interface. The manipulation leads to denial of service. The attack can only be initiated within the local network. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-221552. **CVE ID : CVE-2023-0936**		
Product: tl-wr940n_firmware					
Affected Version(s): 6_3.19.1					
Use of a Broken or Risky Cryptographic Algorithm	22-Feb-2023	7.5	TP-Link router TL-WR940N V6 3.19.1 Build 180119 uses a deprecated MD5 algorithm to hash the admin password used for basic authentication. **CVE ID : CVE-2023-23040**	https://midist0xf.medium.com/tl-wr940n-uses-weak-md5-hashing-algorithm-ae7b589860d2	O-TP--TL-W-170323/1392
Vendor: ui					
Product: unifi_dream_machine_pro_firmware					
Affected Version(s): 7.2.95					
N/A	23-Feb-2023	9.8	Ubiquiti Networks UniFi Dream Machine Pro v7.2.95 allows attackers to bypass domain	N/A	O-UI-UNIF-170323/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restrictions via crafted packets. **CVE ID : CVE-2023-24104**		
Vendor: Zyxel					
Product: lte3202-m437_firmware					
Affected Version(s): 1.00\\(abwf.1\\)c0					
N/A	21-Feb-2023	9.8	A security misconfiguration vulnerability exists in the Zyxel LTE3316-M604 firmware version V2.00(ABMP.6)C0 due to a factory default misconfiguration intended for testing purposes. A remote attacker could leverage this vulnerability to access an affected device using Telnet. **CVE ID : CVE-2023-22920**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-security-misconfiguration-vulnerability-of-4g-lte-indoor-routers	O-ZYX-LTE3-170323/1394
Product: lte3316-m604_firmware					
Affected Version(s): 2.00\\(abmp.6\\)c0					
N/A	21-Feb-2023	9.8	A security misconfiguration vulnerability exists in the Zyxel LTE3316-M604 firmware version V2.00(ABMP.6)C0 due to a factory default misconfiguration intended for testing purposes. A remote attacker could	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-security-misconfiguration-vulnerability-of-4g-lte-	O-ZYX-LTE3-170323/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to access an affected device using Telnet. **CVE ID : CVE-2023-22920**	indoor-routers	