National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 - 31 Jan 2023 Vol. 10 No. 02

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: Adobe					
Product: acrobat					
Affected Version(s): From (including) 20.001.30005 Up to (including) 20.005.30418					
Integer Overflow or Wraparound	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound 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-2023-21579**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/1
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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/acrobat/apsb23-01.html	A-ADO-ACRO-020223/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-21604**		
Heap-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21605**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/3
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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/acrobat/apsb23-01.html	A-ADO-ACRO-020223/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21606		
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21607**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/5
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21608**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21609**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/7
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21610**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/8
Exposure of Resource	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-020223/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21611**	ts/acrobat/apsb23-01.html	
Creation of Temporary File in Directory with Insecure Permissions	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21612**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21581**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/11
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21585**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21613**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/13
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21614**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: acrobat_dc					
Affected Version(s): From (including) 15.008.20082 Up to (including) 22.003.20281					
Integer Overflow or Wraparound	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound 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-2023-21579**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/15
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21604**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Heap-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21605**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/17
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21606**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/18
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-020223/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30418 (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-2023-21607**	ts/acrobat/apsb23-01.html	
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21608**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/20
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-21609**		
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21610**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/22
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in privilege escalation 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-2023-21611**		
Creation of Temporary File in Directory with Insecure Permissions	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21612**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/24
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-21581**		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21585**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/26
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-21613**		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21614**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/28
Affected Version(s): From (including) 15.008.20082 Up to (including) 22.003.20282					
Integer Overflow or Wraparound	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/29

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-2023-21579**		
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21604**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/30
Heap-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/31

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-2023-21605**		
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21606**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/32
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-21607**		
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21608**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/34
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21609**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21610**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/36
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21611**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Creation of Temporary File in Directory with Insecure Permissions	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21612**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/38
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21581**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21585**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/40
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21613**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21614**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/42
Product: acrobat_reader					
Affected Version(s): From (including) 20.001.30005 Up to (including) 20.005.30418					
Integer Overflow or Wraparound	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound 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/acrobat/apsb23-01.html	A-ADO-ACRO-020223/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21579		
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21604**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/44
Heap-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21605**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21606**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/46
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21607**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/47
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-020223/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30418 (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-2023-21608**	ts/acrobat/apsb23-01.html	
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21609**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/49
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-21610**		
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21611**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/51
Creation of Temporary File in Directory with Insecure Permissions	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21612**		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21581**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/53
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-21585**		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21613**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/55
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-21614**		
Product: acrobat_reader_dc					
Affected Version(s): From (including) 15.008.20082 Up to (including) 22.003.20281					
Integer Overflow or Wraparound	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound 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-2023-21579**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/57
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability that could result in	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/58

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-2023-21604**		
Heap-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21605**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/59
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/60

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-2023-21606**		
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21607**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/61
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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/acrobat/apsb23-01.html	A-ADO-ACRO-020223/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-21608**		
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21609**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/63
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21610		
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21611**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/65
Creation of Temporary File in Directory with Insecure Permissions	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-21612**		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21581**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/67
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-21585**		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21613**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/69
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-21614**		
Affected Version(s): From (including) 15.008.20082 Up to (including) 22.003.20282					
Integer Overflow or Wraparound	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound 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-2023-21579**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/71
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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/acrobat/apsb23-01.html	A-ADO-ACRO-020223/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-21604**		
Heap-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21605**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/73
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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/acrobat/apsb23-01.html	A-ADO-ACRO-020223/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21606		
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21607**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/75
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21608**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21609**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/77
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21610**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/78
Exposure of Resource	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx.adobe.com/security/produc	A-ADO-ACRO-020223/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21611**	ts/acrobat/apsb23-01.html	
Creation of Temporary File in Directory with Insecure Permissions	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21612**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21581**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/81
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21585**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21613**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/83
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21614**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	A-ADO-ACRO-020223/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dimension					
Affected Version(s): * Up to (including) 3.4.6					
Use After Free	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (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-2023-21601**	https://helpx.adobe.com/security/products/dimension/apsb23-10.html	A-ADO-DIME-020223/85
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-21603**	https://helpx.adobe.com/security/products/dimension/apsb23-10.html	A-ADO-DIME-020223/86
Vendor: amano					
Product: xoffice					
Affected Version(s): 7.1.3879					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jan-2023	9.8	Amano Xoffice parking solutions 7.1.3879 is vulnerable to SQL Injection. **CVE ID : CVE-2023-23331**	N/A	A-AMA-XOFF-020223/87
Vendor: Apache					
Product: airflow					
Affected Version(s): * Up to (excluding) 2.5.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Jan-2023	9.8	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Software Foundation Apache Airflow, Apache Software Foundation Apache Airflow MySQL Provider.This issue affects Apache Airflow: before 2.5.1; Apache Airflow MySQL Provider: before 4.0.0. **CVE ID : CVE-2023-22884**	https://github.com/apache/airflow/pull/28811	A-APA-AIRF-020223/88
Product: airflow_mysql_provider					
Affected Version(s): * Up to (excluding) 4.0.0					
Improper Neutralization of Special Elements used in a Command ('Comman	21-Jan-2023	9.8	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Software Foundation Apache Airflow, Apache Software Foundation	https://github.com/apache/airflow/pull/28811	A-APA-AIRF-020223/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			Apache Airflow MySQL Provider.This issue affects Apache Airflow: before 2.5.1; Apache Airflow MySQL Provider: before 4.0.0. **CVE ID : CVE-2023-22884**		
Vendor: asynchttpclient_project					
Product: async-http-client					
Affected Version(s): * Up to (excluding) 1.4.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-Jan-2023	7.5	Versions of Async HTTP Client prior to 1.13.2 are vulnerable to a form of targeted request manipulation called CRLF injection. This vulnerability was the result of insufficient validation of HTTP header field values before sending them to the network. Users are vulnerable if they pass untrusted data into HTTP header field values without prior sanitisation. Common use-cases here might be to place usernames from a database into HTTP header fields. This vulnerability allows attackers to inject new HTTP header fields, or entirely new requests, into the data stream. This can cause requests to be understood very differently by the remote server than was	N/A	A-ASY-ASYN-020223/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intended. In general, this is unlikely to result in data disclosure, but it can result in a number of logical errors and other misbehaviours. **CVE ID : CVE-2023-0040**		
Affected Version(s): From (including) 1.10.0 Up to (excluding) 1.12.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-Jan-2023	7.5	Versions of Async HTTP Client prior to 1.13.2 are vulnerable to a form of targeted request manipulation called CRLF injection. This vulnerability was the result of insufficient validation of HTTP header field values before sending them to the network. Users are vulnerable if they pass untrusted data into HTTP header field values without prior sanitisation. Common use-cases here might be to place usernames from a database into HTTP header fields. This vulnerability allows attackers to inject new HTTP header fields, or entirely new requests, into the data stream. This can cause requests to be understood very differently by the remote server than was intended. In general, this is unlikely to result in data disclosure, but it	N/A	A-ASY-ASYN-020223/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can result in a number of logical errors and other misbehaviours. **CVE ID : CVE-2023-0040**		
Affected Version(s): From (including) 1.13.0 Up to (excluding) 1.13.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-Jan-2023	7.5	Versions of Async HTTP Client prior to 1.13.2 are vulnerable to a form of targeted request manipulation called CRLF injection. This vulnerability was the result of insufficient validation of HTTP header field values before sending them to the network. Users are vulnerable if they pass untrusted data into HTTP header field values without prior sanitisation. Common use-cases here might be to place usernames from a database into HTTP header fields. This vulnerability allows attackers to inject new HTTP header fields, or entirely new requests, into the data stream. This can cause requests to be understood very differently by the remote server than was intended. In general, this is unlikely to result in data disclosure, but it can result in a number of logical errors and other misbehaviours.	N/A	A-ASY-ASYN-020223/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0040		
Affected Version(s): From (including) 1.5.0 Up to (excluding) 1.9.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-Jan-2023	7.5	Versions of Async HTTP Client prior to 1.13.2 are vulnerable to a form of targeted request manipulation called CRLF injection. This vulnerability was the result of insufficient validation of HTTP header field values before sending them to the network. Users are vulnerable if they pass untrusted data into HTTP header field values without prior sanitisation. Common use-cases here might be to place usernames from a database into HTTP header fields. This vulnerability allows attackers to inject new HTTP header fields, or entirely new requests, into the data stream. This can cause requests to be understood very differently by the remote server than was intended. In general, this is unlikely to result in data disclosure, but it can result in a number of logical errors and other misbehaviours. **CVE ID : CVE-2023-0040**	N/A	A-ASY-ASYN-020223/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ays-pro					
Product: survey_maker					
Affected Version(s): * Up to (excluding) 3.1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-2023	8.8	The Survey Maker WordPress Plugin, version < 3.1.2, is affected by an authenticated SQL injection vulnerability in the 'surveys_ids' parameter of its 'ays_surveys_export_json' action. **CVE ID : CVE-2023-23490**	N/A	A-AYS-SURV-020223/94
Vendor: book_store_management_system_project					
Product: book_store_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	Book Store Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in /bsms_ci/index.php/book. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the writer parameter. **CVE ID : CVE-2023-23024**	N/A	A-BOO-BOOK-020223/95
Vendor: builder					
Product: qwik					
Affected Version(s): * Up to (excluding) 0.16.2					
Improper Neutralizat	20-Jan-2023	6.1	Cross-site Scripting (XSS) - Generic in	https://huntr.dev/bounties	A-BUI-QWIK-020223/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			GitHub repository builderio/qwik prior to 0.1.0-beta5. **CVE ID : CVE-2023-0410**	/2da583f0-7f66-4ba7-9bed-8e7229aa578e, https://github.com/builderio/qwik/commit/4b2f89dbbd2bc0a2c92eae1a49bdd186e589151a	
Vendor: Cakephp					
Product: cakephp					
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.12					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2023	9.8	CakePHP is a development framework for PHP web apps. In affected versions the `Cake\Database\Query::limit()` and `Cake\Database\Query::offset()` methods are vulnerable to SQL injection if passed un-sanitized user request data. This issue has been fixed in 4.2.12, 4.3.11, 4.4.10. Users are advised to upgrade. Users unable to upgrade may mitigate this issue by using CakePHP's Pagination library. Manually validating or casting parameters to these methods will also mitigate the issue. **CVE ID : CVE-2023-22727**	https://bakery.cakephp.org/2023/01/06/cakephp_4211_4311_4410_released.html, https://github.com/cakephp/cakephp/commit/3f463e7084b5a15e67205ced3a622577cca7a239	A-CAK-CAKE-020223/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.3.11					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2023	9.8	CakePHP is a development framework for PHP web apps. In affected versions the `Cake\Database\Query::limit()` and `Cake\Database\Query::offset()` methods are vulnerable to SQL injection if passed un-sanitized user request data. This issue has been fixed in 4.2.12, 4.3.11, 4.4.10. Users are advised to upgrade. Users unable to upgrade may mitigate this issue by using CakePHP's Pagination library. Manually validating or casting parameters to these methods will also mitigate the issue. **CVE ID : CVE-2023-22727**	https://bakery.cakephp.org/2023/01/06/cakephp_4211_4311_4410_released.html, https://github.com/cakephp/cakephp/commit/3f463e7084b5a15e67205ced3a622577cca7a239	A-CAK-CAKE-020223/98
Affected Version(s): From (including) 4.4.0 Up to (excluding) 4.4.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2023	9.8	CakePHP is a development framework for PHP web apps. In affected versions the `Cake\Database\Query::limit()` and `Cake\Database\Query::offset()` methods are vulnerable to SQL injection if passed un-sanitized user request data. This issue has been fixed in 4.2.12,	https://bakery.cakephp.org/2023/01/06/cakephp_4211_4311_4410_released.html, https://github.com/cakephp/cakephp/commit/3f463e7084b5a15e67205ced3a62	A-CAK-CAKE-020223/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.3.11, 4.4.10. Users are advised to upgrade. Users unable to upgrade may mitigate this issue by using CakePHP's Pagination library. Manually validating or casting parameters to these methods will also mitigate the issue. **CVE ID : CVE-2023-22727**	2577cca7a239	
Vendor: Cisco					
Product: cx_cloud_agent					
Affected Version(s): * Up to (excluding) 1.9					
Incorrect Default Permissions	20-Jan-2023	6.7	A vulnerability in Cisco CX Cloud Agent of could allow an authenticated, local attacker to elevate their privileges. This vulnerability is due to insecure file permissions. An attacker could exploit this vulnerability by calling the script with sudo. A successful exploit could allow the attacker to take complete control of the affected device. **CVE ID : CVE-2023-20043**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cxagent-gOq9QjqZ	A-CIS-CX_C-020223/100
Affected Version(s): * Up to (excluding) 2.2.1					
N/A	20-Jan-2023	7.3	A vulnerability in Cisco CX Cloud Agent of could allow an authenticated, local attacker to elevate their privileges. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	A-CIS-CX_C-020223/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insecure file permissions. An attacker could exploit this vulnerability by persuading support to update settings which call the insecure script. A successful exploit could allow the attacker to take complete control of the affected device. **CVE ID : CVE-2023-20044**	sco-sa-cxagent-gOq9QjqZ	
Affected Version(s): 2.2					
Incorrect Default Permissions	20-Jan-2023	6.7	A vulnerability in Cisco CX Cloud Agent of could allow an authenticated, local attacker to elevate their privileges. This vulnerability is due to insecure file permissions. An attacker could exploit this vulnerability by calling the script with sudo. A successful exploit could allow the attacker to take complete control of the affected device. **CVE ID : CVE-2023-20043**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cxagent-gOq9QjqZ	A-CIS-CX_C-020223/102
Product: industrial_network_director					
Affected Version(s): * Up to (excluding) 1.6.0					
Use of Hard-coded Credentials	20-Jan-2023	8.8	A vulnerability in the monitoring application of Cisco Industrial Network Director could allow an authenticated, local attacker to access a static secret key used	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	A-CIS-INDU-020223/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to store both local data and credentials for accessing remote systems. This vulnerability is due to a static key value stored in the application used to encrypt application data and remote credentials. An attacker could exploit this vulnerability by gaining local access to the server Cisco Industrial Network Director is installed on. A successful exploit could allow the attacker to decrypt data allowing the attacker to access remote systems monitored by Cisco Industrial Network Director. **CVE ID : CVE-2023-20038**	sco-sa-ind-fZyVjJtG	
Affected Version(s): * Up to (excluding) 1.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	5.4	A vulnerability in Cisco Industrial Network Director could allow an authenticated, remote attacker to conduct stored cross-site scripting (XSS) attacks. The vulnerability is due to improper validation of content submitted to the affected application. An attacker could exploit this vulnerability by sending requests containing malicious	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ind-fZyVjJtG	A-CIS-INDU-020223/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			values to the affected system. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20037**		
Product: network_services_orchestrator					
Affected Version(s): 5.8					
Unrestricted Upload of File with Dangerous Type	20-Jan-2023	5.5	A vulnerability in the NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-zjBeMkZg	A-CIS-NETW-020223/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless the --run-as-user option is used. **CVE ID : CVE-2023-20040**		
Affected Version(s): From (including) 3.3 Up to (excluding) 5.4.7					
Unrestricted Upload of File with Dangerous Type	20-Jan-2023	5.5	A vulnerability in the NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-zjBeMkZg	A-CIS-NETW-020223/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless the --run-as-user option is used. **CVE ID : CVE-2023-20040**		
Affected Version(s): From (including) 5.5 Up to (excluding) 5.5.6					
Unrestricted Upload of File with Dangerous Type	20-Jan-2023	5.5	A vulnerability in the NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-zjBeMkZg	A-CIS-NETW-020223/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless the --run-as-user option is used. **CVE ID : CVE-2023-20040**		
Affected Version(s): From (including) 5.6 Up to (excluding) 5.6.7					
Unrestricted Upload of File with Dangerous Type	20-Jan-2023	5.5	A vulnerability in the NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-zjBeMkZg	A-CIS-NETW-020223/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless the --run-as-user option is used. **CVE ID : CVE-2023-20040**		
Affected Version(s): From (including) 5.7 Up to (excluding) 5.7.4					
Unrestricted Upload of File with Dangerous Type	20-Jan-2023	5.5	A vulnerability in the NETCONF service of Cisco Network Services Orchestrator (NSO) could allow an authenticated, remote attacker to cause a denial of service (DoS) on an affected system that is running as the root user. To exploit this vulnerability, the attacker must be a member of the admin group. This vulnerability exists because user-supplied input is not properly validated when NETCONF is used to upload packages to an affected device. An attacker could exploit this vulnerability by uploading a specially crafted package file. A successful exploit could allow the attacker to write crafted files to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-zjBeMkZg	A-CIS-NETW-020223/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary locations on the filesystem or delete arbitrary files from the filesystem of an affected device, resulting in a DoS condition. Note: By default, during install, Cisco NSO will be set up to run as the root user unless the --run-as-user option is used. **CVE ID : CVE-2023-20040**		
Product: sip_ip_phone_software					
Affected Version(s): * Up to (including) 1.2.0					
Allocation of Resources Without Limits or Throttling	20-Jan-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lldp-memlk-McOecPT	A-CIS-SIP_-020223/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. **CVE ID : CVE-2023-20047**		
Product: telepresence_collaboration_endpoint					
Affected Version(s): 8.0.0					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/111
Affected Version(s): 8.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/112
Affected Version(s): 8.1.0					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Affected Version(s): 8.1.1					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/114
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-TELE-020223/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	ityAdvisory/cisco-sa-roomos-dkjGFgRK	
Affected Version(s): 8.2.0					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Affected Version(s): 8.2.1					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/117
Affected Version(s): 8.2.2					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Affected Version(s): 8.3.0					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20008		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/120
Affected Version(s): 8.3.1					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Affected Version(s): 8.3.2					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/122
Affected Version(s): 8.3.3					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and	https://sec.cloudapps.cisco.com/security	A-CIS-TELE-020223/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	
Affected Version(s): 8.3.5					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/125
Affected Version(s): 8.3.6					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Affected Version(s): 9.0.1					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20008		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/128
Affected Version(s): 9.1.1					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/130
Affected Version(s): 9.1.2					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-TELE-020223/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	ityAdvisory/cisco-sa-roomos-dkjGFgRK	
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 9.1.3					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/133
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 9.1.4					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/136
Affected Version(s): 9.1.5					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/138
Affected Version(s): 9.1.6					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-TELE-020223/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	roomos-dkjGFgRK	
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20002		
Affected Version(s): 9.10.1					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/141
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 9.10.2					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/143
Server-Side Request	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/conte	A-CIS-TELE-020223/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	nt/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	
Affected Version(s): 9.10.3					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/146
Affected Version(s): 9.12.3					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/148
Affected Version(s): 9.12.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/149
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 9.12.5					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/151
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-TELE-020223/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	roomos-dkjGFgRK	
Affected Version(s): 9.13.0					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20008		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/154
Affected Version(s): 9.13.1					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/156
Affected Version(s): 9.13.2					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-TELE-020223/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	ityAdvisory/cisco-sa-roomos-dkjGFgRK	
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 9.13.3					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/159
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 9.14.3					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/162
Affected Version(s): 9.14.4					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/164
Affected Version(s): 9.14.5					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-TELE-020223/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	roomos-dkjGFgRK	
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20002		
Affected Version(s): 9.14.6					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/167
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 9.15.0.10					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/169
Server-Side Request	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/conte	A-CIS-TELE-020223/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	nt/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	
Affected Version(s): 9.15.0.11					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/172
Affected Version(s): 9.15.10.8					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/174
Affected Version(s): 9.15.13.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/175
Affected Version(s): 9.15.3.25					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/177
Affected Version(s): 9.15.3.26					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	A-CIS-TELE-020223/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	sco-sa-roomos-dkjGFgRK	
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20002		
Affected Version(s): 9.15.8.12					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/180
Affected Version(s): 9.2.1					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/182
Affected Version(s): 9.2.2					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco	https://sec.cloudapps.cisco	A-CIS-TELE-020223/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 9.2.3					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/185
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 9.2.4					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20008		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/188
Affected Version(s): 9.9.3					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/190
Affected Version(s): 9.9.4					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-TELE-020223/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	ityAdvisory/cisco-sa-roomos-dkjGFgRK	
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sourced from the affected system. **CVE ID : CVE-2023-20002**		
Product: telepresence_tc					
Affected Version(s): 7.3.13					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/193
Affected Version(s): 7.3.21					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-TELE-020223/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	roomos-dkjGFgRK	
Affected Version(s): 7.3.5					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20008		
Affected Version(s): 7.3.6					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/196
Affected Version(s): 7.3.7					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Affected Version(s): 7.3.9					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	A-CIS-TELE-020223/198
Product: unified_communications_manager					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 12.5\\(1\\)su7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-2023	8.8	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low-privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read or modify any data on the underlying database or elevate their privileges. **CVE ID : CVE-2023-20010**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-sql-rpPczR8n	A-CIS-UNIF-020223/199
Affected Version(s): From (including) 11.5\\(1\\) Up to (excluding) 12.5\\(1\\)su7					
Improper Neutralization of Special Elements	20-Jan-2023	8.8	A vulnerability in the web-based management interface of Cisco Unified Communications	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	A-CIS-UNIF-020223/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low-privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read or modify any data on the underlying database or elevate their privileges. **CVE ID : CVE-2023-20010**	ityAdvisory/cisco-sa-cucm-sql-rpPczR8n	
Affected Version(s): From (including) 14.0 Up to (excluding) 14su2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-2023	8.8	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-sql-rpPczR8n	A-CIS-UNIF-020223/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low-privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read or modify any data on the underlying database or elevate their privileges. **CVE ID : CVE-2023-20010**		
Vendor: classroombookings					
Product: classroombookings					
Affected Version(s): 2.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	Cross Site Scripting (XSS) vulnerability in craigrodway classroombookings 2.6.4 allows attackers to execute arbitrary code or other unspecified impacts via the input bgcol in file Weeks.php. **CVE ID : CVE-2023-23012**	N/A	A-CLA-CLAS-020223/202
Vendor: contec					
Product: conprosys_hmi_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 3.4.5					
Improper Privilege Management	20-Jan-2023	7.5	Use of default credentials vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote unauthenticated attacker to alter user credentials information. **CVE ID : CVE-2023-22331**	https://jvn.jp/en/vu/JVNVU96873821, https://www.contec.com/download/contract/contract4/?itemid=ea8039aa-3434-4999-9ab6-897aa690210c&downloaditemid=866d7d3c-aae9-438d-87f3-17aa040df90b	A-CON-CONP-020223/203
N/A	20-Jan-2023	7.5	Improper access control vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote unauthenticated attacker to bypass access restriction and obtain the server certificate including the private key of the product. **CVE ID : CVE-2023-22339**	https://jvn.jp/en/vu/JVNVU96873821, https://www.contec.com/download/contract/contract4/?itemid=ea8039aa-3434-4999-9ab6-897aa690210c&downloaditemid=866d7d3c-aae9-438d-87f3-17aa040df90b	A-CON-CONP-020223/204
Improper Neutralization of Input During Web Page Generation	20-Jan-2023	5.4	Cross-site scripting vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote authenticated attacker to inject an arbitrary script and	https://jvn.jp/en/vu/JVNVU96873821, https://www.contec.com/download/contract/contract4/?itemid=ea	A-CON-CONP-020223/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			obtain the sensitive information. **CVE ID : CVE-2023-22373**	8039aa-3434-4999-9ab6-897aa690210c&downloaditemid=866d7d3c-aae9-438d-87f3-17aa040df90b	
Improper Authentication	20-Jan-2023	5.3	Use of password hash instead of password for authentication vulnerability in CONPROSYS HMI System (CHS) Ver.3.4.5 and earlier allows a remote authenticated attacker to obtain user credentials information via a man-in-the-middle attack. **CVE ID : CVE-2023-22334**	https://jvn.jp/en/vu/JVNVU96873821, https://www.contec.com/download/contract/contract4/?itemid=ea8039aa-3434-4999-9ab6-897aa690210c&downloaditemid=866d7d3c-aae9-438d-87f3-17aa040df90b	A-CON-CONP-020223/206
Vendor: custom_404_pro_project					
Product: custom_404_pro					
Affected Version(s): * Up to (excluding) 3.7.2					
Cross-Site Request Forgery (CSRF)	18-Jan-2023	4.3	The Custom 404 Pro plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.7.1. This is due to missing or incorrect nonce validation on the custom_404_pro_admin_init function. This makes it possible for unauthenticated	https://plugins.trac.wordpress.org/browser/custom-404-pro/tags/3.7.1/admin/AdminClass.php#L114, https://www.wordfence.com/threat-intel/vulnera	A-CUS-CUST-020223/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to delete logs, via forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-0385**	bilities/id/968920b9-febf-4d76-a16b-f27954cd72e5	
Vendor: daj					
Product: m-filter					
Affected Version(s): From (including) 4.0 Up to (excluding) 4.87r04					
N/A	17-Jan-2023	5.3	m-FILTER prior to Ver.5.70R01 (Ver.5 Series) and m-FILTER prior to Ver.4.87R04 (Ver.4 Series) allows a remote unauthenticated attacker to bypass authentication and send users' unintended email when email is being sent under the certain conditions. The attacks exploiting this vulnerability have been observed. **CVE ID : CVE-2023-22278**	N/A	A-DAJ-M-FI-020223/208
Affected Version(s): From (including) 5.0 Up to (excluding) 5.70r01					
N/A	17-Jan-2023	5.3	m-FILTER prior to Ver.5.70R01 (Ver.5 Series) and m-FILTER prior to Ver.4.87R04 (Ver.4 Series) allows a remote unauthenticated attacker to bypass authentication and send users' unintended email when email is being sent under the certain	N/A	A-DAJ-M-FI-020223/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			conditions. The attacks exploiting this vulnerability have been observed. **CVE ID : CVE-2023-22278**		
Vendor: daloradius					
Product: daloradius					
Affected Version(s): * Up to (excluding) 2023-01-18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository lirantal/daloradius prior to master-branch. **CVE ID : CVE-2023-0337**	https://huntr.dev/bounties/1c50a5a5-3f55-4b6f-b861-4d5cdb6eb81b, https://github.com/lirantal/daloradius/commit/e77a769c7503e63a2e3c05262cb5f8f81a4a7bbe	A-DAL-DALO-020223/210
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository lirantal/daloradius prior to master-branch. **CVE ID : CVE-2023-0338**	https://huntr.dev/bounties/fcae1b67-db37-4d24-9137-8dda95573e77, https://github.com/lirantal/daloradius/commit/e77a769c7503e63a2e3c05262cb5f8f81a4a7bbe	A-DAL-DALO-020223/211
Vendor: Dell					
Product: cloud_mobility_for_dell_emc_storage					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.3.4.0					
Improper Certificate Validation	19-Jan-2023	7	Cloud Mobility for Dell EMC Storage, versions 1.3.0.X and below contains an Improper Check for Certificate Revocation vulnerability. A threat actor does not need any specific privileges to potentially exploit this vulnerability. An attacker could perform a man-in-the-middle attack and eavesdrop on encrypted communications from Cloud Mobility to Cloud Storage devices. Exploitation could lead to the compromise of secret and sensitive information, cloud storage connection downtime, and the integrity of the connection to the Cloud devices. **CVE ID : CVE-2023-23690**	https://www.dell.com/support/kbdoc/en-us/000207521/dsa-2023-019-dell-emc-cloud-mobility-security-update-for-certificate-revocation-vulnerability	A-DEL-CLOU-020223/212
Vendor: deno					
Product: deno					
Affected Version(s): From (including) 1.9.0 Up to (excluding) 1.29.3					
Concurrent Execution using Shared Resource with Improper Synchronization	17-Jan-2023	7.5	Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Multi-threaded programs were able to spoof interactive permission prompt by rewriting the prompt to	https://github.com/denoland/deno/pull/17392	A-DEN-DENO-020223/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			suggest that program is waiting on user confirmation to unrelated action. A malicious program could clear the terminal screen after permission prompt was shown and write a generic message. This situation impacts users who use Web Worker API and relied on interactive permission prompt. The reproduction is very timing sensitive and can't be reliably reproduced on every try. This problem can not be exploited on systems that do not attach an interactive prompt (for example headless servers). The problem has been fixed in Deno v1.29.3; it is recommended all users update to this version. Users are advised to upgrade. Users unable to upgrade may run with --no-prompt flag to disable interactive permission prompts. **CVE ID : CVE-2023-22499**		
Vendor: devolutions					
Product: remote_desktop_manager					
Affected Version(s): 2022.3.29					
N/A	26-Jan-2023	3.3	The force offline MFA prompt setting is not respected when	https://devolutions.net/security/advisori	A-DEV-REMO-020223/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			switching to offline mode in Devolutions Remote Desktop Manager 2022.3.29 to 2022.3.30 allows a user to save sensitive data on disk. **CVE ID : CVE-2023-0463**	es/DEVO-2023-0001	
Affected Version(s): 2022.3.30					
N/A	26-Jan-2023	3.3	The force offline MFA prompt setting is not respected when switching to offline mode in Devolutions Remote Desktop Manager 2022.3.29 to 2022.3.30 allows a user to save sensitive data on disk. **CVE ID : CVE-2023-0463**	https://devolutions.net/security/advisories/DEVO-2023-0001	A-DEV-REMO-020223/215
Vendor: e-dynamics					
Product: events_made_easy					
Affected Version(s): * Up to (including) 2.3.16					
Missing Authorization	19-Jan-2023	5.4	The Events Made Easy plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on several functions related to AJAX actions in versions up to, and including, 2.3.16. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to invoke those functions intended for	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2836308%40events-made-easy&new=2836308%40events-made-easy&sfp_email=&sfph_mail=	A-E-D-EVEN-020223/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator use. While the plugin is still pending review from the WordPress repository, site owners can download a copy of the patched version directly from the developer's Github at https://github.com/liedekef/events-made-easy **CVE ID : CVE-2023-0404**		
Vendor: ecommerce-codeigniter-bootstrap_project					
Product: ecommerce-codeigniter-bootstrap					
Affected Version(s): * Up to (excluding) 2022-12-27					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	Cross Site Scripting (XSS) vulnerability in Ecommerce-CodeIgniter-Bootstrap thru commit d5904379ca55014c5df34c67deda982c73dc7fe5 (on Dec 27, 2022), allows attackers to execute arbitrary code via the languages and trans_load parameters in file add_product.php. **CVE ID : CVE-2023-23010**	https://github.com/kirilkirkov/Ecommerce-CodeIgniter-Bootstrap/commit/d5904379ca55014c5df34c67deda982c73dc7fe5, https://github.com/kirilkirkov/Ecommerce-CodeIgniter-Bootstrap/issues/242, https://gist.github.com/enferas/8a836008e9f635a2f80d09c9a8b5a533	A-ECO-ECOM-020223/217
Vendor: Froxlor					
Product: froxlor					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.0.0					
Path Traversal: '..filename'	16-Jan-2023	5.5	Path Traversal: '\..\filename' in GitHub repository froxlor/froxlor prior to 2.0.0. **CVE ID : CVE-2023-0316**	https://github.com/froxlor/froxlor/commit/983d92946039250182 25d672795bd 8b4a526f41e, https://huntr.dev/bounties/c190e42a-4806-47aa-aa1e-ff5d6407e244	A-FRO-FROX-020223/218
Affected Version(s): * Up to (excluding) 2.0.8					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jan-2023	8.8	Command Injection in GitHub repository froxlor/froxlor prior to 2.0.8. **CVE ID : CVE-2023-0315**	https://huntr.dev/bounties/ff4e177b-ba48-4913-bbfa-ab8ce0db5943, https://github.com/froxlor/froxlor/commit/090cfc26f2722ac3036cc7fd1861955bc36f065a	A-FRO-FROX-020223/219
Vendor: fullworksplugins					
Product: quick_event_manager					
Affected Version(s): * Up to (excluding) 9.7.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	The Quick Event Manager WordPress Plugin, version < 9.7.5, is affected by a reflected cross-site scripting vulnerability in the 'category' parameter of its 'qem_ajax_calendar' action.	N/A	A-FUL-QUIC-020223/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23491		
Vendor: Glpi-project					
Product: glpi					
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.6					
Incorrect Authorization	26-Jan-2023	7.5	GLPI is a Free Asset and IT Management Software package. Versions 10.0.0 and above, prior to 10.0.6 are vulnerable to Incorrect Authorization. This vulnerability allow unauthorized access to inventory files. Thus, if anonymous access to FAQ is allowed, inventory files are accessbile by unauthenticated users. This issue is patched in version 10.0.6. As a workaround, disable native inventory and delete inventory files from server (default location is `files/_inventory`). **CVE ID : CVE-2023-22500**	N/A	A-GLP-GLPI-020223/221
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2023	6.1	GLPI is a Free Asset and IT Management Software package. Versions 9.4.0 and above, prior to 10.0.6 are subject to Cross-site Scripting. An attacker can persuade a victim into opening a URL containing a payload exploiting this vulnerability. After	N/A	A-GLP-GLPI-020223/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploited, the attacker can make actions as the victim or exfiltrate session cookies. This issue is patched in version 10.0.6. **CVE ID : CVE-2023-22722**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2023	4.8	GLPI is a Free Asset and IT Management Software package. Versions prior to 10.0.6 are subject to Cross-site Scripting via malicious RSS feeds. An Administrator can import a malicious RSS feed that contains Cross Site Scripting (XSS) payloads inside RSS links. Victims who wish to visit an RSS content and click on the link will execute the Javascript. This issue is patched in 10.0.6. **CVE ID : CVE-2023-22724**	N/A	A-GLP-GLPI-020223/223
Affected Version(s): From (including) 9.4.0 Up to (excluding) 9.5.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2023	6.1	GLPI is a Free Asset and IT Management Software package. Versions 9.4.0 and above, prior to 10.0.6 are subject to Cross-site Scripting. An attacker can persuade a victim into opening a URL containing a payload exploiting this vulnerability. After exploited, the attacker	N/A	A-GLP-GLPI-020223/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can make actions as the victim or exfiltrate session cookies. This issue is patched in version 10.0.6. **CVE ID : CVE-2023-22722**		
Vendor: gpac					
Product: gpac					
Affected Version(s): * Up to (including) 2.2.0					
Use After Free	18-Jan-2023	7.8	Use After Free in GitHub repository gpac/gpac prior to 2.3.0-DEV. **CVE ID : CVE-2023-0358**	https://huntr.dev/bounties/93e128ed-253f-4c42-81ff-fbac7fd8f355, https://github.com/gpac/gpac/commit/9971fb125cf91cefd081a080c417b90bbe4a467b	A-GPA-GPAC-020223/225
Affected Version(s): 2.2-rev0-gab012bbfb-master					
Missing Release of Memory after Effective Lifetime	20-Jan-2023	7.8	GPAC version 2.2-rev0-gab012bbfb-master was discovered to contain a memory leak in lsr_read_rare_full function. **CVE ID : CVE-2023-23145**	https://github.com/gpac/gpac/commit/4ade98128cbc41d5115b97a41ca2e59529c8dd5f	A-GPA-GPAC-020223/226
Integer Overflow or Wraparound	20-Jan-2023	5.5	Integer overflow vulnerability in function Q_DecCoordOnUnitSphere file bifs/unquantize.c in GPAC version 2.2-rev0-gab012bbfb-master.	https://github.com/gpac/gpac/commit/3a2458a49b3e6399709d456d7b35e7a6f50cfb86	A-GPA-GPAC-020223/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23144		
Affected Version(s): 2.3-dev-rev1-g4669ba229-master					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jan-2023	7.8	Buffer overflow vulnerability in function avc_parse_slice in file media_tools/av_parsers.c. GPAC version 2.3-DEV-rev1-g4669ba229-master. **CVE ID : CVE-2023-23143**	https://github.com/gpac/gpac/commit/af6a5e7a96ee01a139cce6c9e4edfc069aad17a6	A-GPA-GPAC-020223/228
Vendor: healthchecks					
Product: healthchecks					
Affected Version(s): * Up to (excluding) 2.6					
Observable Discrepancy	23-Jan-2023	5.3	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository healthchecks/healthchecks prior to v2.6. **CVE ID : CVE-2023-0440**	https://huntr.dev/bounties/208a096f-7986-4eed-8629-b7285348a686, https://github.com/healthchecks/healthchecks/commit/359edbd2709e27b60687061a32e19322bc971c1f	A-HEA-HEAL-020223/229
Vendor: html-stripscripts_project					
Product: html-stripscripts					
Affected Version(s): * Up to (including) 1.06					
N/A	21-Jan-2023	7.5	The HTML-StripScripts module through 1.06 for Perl allows _hss_attval_style ReDoS because of catastrophic backtracking for HTML	N/A	A-HTM-HTML-020223/230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			content with certain style attributes. **CVE ID : CVE-2023-24038**		
Vendor: IBM					
Product: qradar_security_information_and_event_manager					
Affected Version(s): 7.4.0					
Exposure of Sensitive Information to an Unauthorized Actor	17-Jan-2023	7.5	IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. **CVE ID : CVE-2023-22875**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244356, https://www.ibm.com/support/pages/node/6855643	A-IBM-QRAD-020223/231
Affected Version(s): 7.5.0					
Exposure of Sensitive Information to an Unauthorized Actor	17-Jan-2023	7.5	IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356. **CVE ID : CVE-2023-22875**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244356, https://www.ibm.com/support/pages/node/6855643	A-IBM-QRAD-020223/232
Product: robotic_process_automation					
Affected Version(s): * Up to (excluding) 21.0.3					
Cleartext Transmission of Sensitive Information	18-Jan-2023	5.9	IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitly	https://www.ibm.com/support/pages/node/6855837, https://exchange.xforce.ib	A-IBM-ROBO-020223/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified in the URL. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 244109. **CVE ID : CVE-2023-22863**	mcloud.com/vulnerabilities/244109	
Affected Version(s): * Up to (excluding) 21.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	5.4	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 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: 244075. **CVE ID : CVE-2023-22594**	https://www.ibm.com/support/pages/node/6855835, https://exchange.xforce.ibmcloud.com/vulnerabilities/244075	A-IBM-ROBO-020223/234
Product: robotic_process_automation_as_a_service					
Affected Version(s): * Up to (excluding) 21.0.3					
Cleartext Transmission of Sensitive Information	18-Jan-2023	5.9	IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitly specified in the URL. This could allow an attacker to obtain sensitive information using man in the middle	https://www.ibm.com/support/pages/node/6855837, https://exchange.xforce.ibmcloud.com/vulnerabilities/244109	A-IBM-ROBO-020223/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			techniques. IBM X-Force ID: 244109. **CVE ID : CVE-2023-22863**		
Affected Version(s): * Up to (excluding) 21.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	5.4	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 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: 244075. **CVE ID : CVE-2023-22594**	https://www.ibm.com/support/pages/node/6855835, https://exchange.xforce.ibmcloud.com/vulnerabilities/244075	A-IBM-ROBO-020223/236
Product: robotic_process_automation_for_cloud_pak					
Affected Version(s): * Up to (excluding) 21.0.3					
Cleartext Transmission of Sensitive Information	18-Jan-2023	5.9	IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitly specified in the URL. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 244109. **CVE ID : CVE-2023-22863**	https://www.ibm.com/support/pages/node/6855837, https://exchange.xforce.ibmcloud.com/vulnerabilities/244109	A-IBM-ROBO-020223/237
Affected Version(s): * Up to (excluding) 21.0.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	5.4	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 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: 244075. **CVE ID : CVE-2023-22594**	https://www.ibm.com/support/pages/node/6855835, https://exchange.xforce.ibmcloud.com/vulnerabilities/244075	A-IBM-ROBO-020223/238
Affected Version(s): From (including) 21.0.1 Up to (excluding) 21.0.5					
Incorrect Permission Assignment for Critical Resource	18-Jan-2023	7.8	IBM Robotic Process Automation for Cloud Pak 21.0.1 through 21.0.4 could allow a local user to perform unauthorized actions due to insufficient permission settings. IBM X-Force ID: 244073. **CVE ID : CVE-2023-22592**	https://www.ibm.com/support/pages/node/6855839, https://exchange.xforce.ibmcloud.com/vulnerabilities/244073	A-IBM-ROBO-020223/239
Vendor: inventory_system_project					
Product: inventory_system					
Affected Version(s): * Up to (including) 2021-04-23					
Improper Neutralization of Input During Web Page Generation	20-Jan-2023	6.1	Cross Site Scripting (XSS) vulnerability in InventorySystem thru commit e08fbbe17902146313501ed0b5feba81d58f455c (on Apr 23, 2021) via edit_store_name and	N/A	A-INV-INVE-020223/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			edit_active inputs in file InventorySystem.php. **CVE ID : CVE-2023-23014**		
Vendor: jc21					
Product: nginx_proxy_manager					
Affected Version(s): * Up to (including) 2.9.19					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	8.8	jc21 NGINX Proxy Manager through 2.9.19 allows OS command injection. When creating an access list, the backend builds an htpasswd file with crafted username and/or password input that is concatenated without any validation, and is directly passed to the exec command, potentially allowing an authenticated attacker to execute arbitrary commands on the system. NOTE: this is not part of any NGINX software shipped by F5. **CVE ID : CVE-2023-23596**	N/A	A-JC2-NGIN-020223/241
Vendor: kalkun_project					
Product: kalkun					
Affected Version(s): 0.8.0					
Improper Neutralization of Input During Web Page Generation	20-Jan-2023	6.1	Cross Site Scripting (XSS) vulnerability in Kalkun 0.8.0 via username input in file User_model.php. **CVE ID : CVE-2023-23015**	https://gist.github.com/enferas/eaf599190451745f1b339f64cca4a36d, https://github.com/kalkun-	A-KAL-KALK-020223/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				sms/Kalkun/issues/487	
Vendor: Keepass					
Product: keepass					
Affected Version(s): * Up to (including) 2.53					
Cleartext Storage of Sensitive Information	22-Jan-2023	5.5	** DISPUTED ** KeePass through 2.53 (in a default installation) allows an attacker, who has write access to the XML configuration file, to obtain the cleartext passwords by adding an export trigger. NOTE: the vendor's position is that the password database is not intended to be secure against an attacker who has that level of access to the local PC. **CVE ID : CVE-2023-24055**	https://sourceforge.net/p/keepass/discussion/329220/thread/a146e5cf6b/	A-KEE-KEEP-020223/243
Vendor: libgit2					
Product: libgit2					
Affected Version(s): * Up to (excluding) 1.4.5					
Improper Verification of Cryptographic Signature	20-Jan-2023	5.9	libgit2 is a cross-platform, linkable library implementation of Git. When using an SSH remote with the optional libssh2 backend, libgit2 does not perform certificate checking by default. Prior versions of libgit2 require the caller to set the `certificate_check` field of libgit2's `git_remote_callbacks`	https://github.com/libgit2/libgit2/commit/42e5db98b963ae503229c63e44e06e439df50e56, https://github.com/libgit2/libgit2/commit/cd6f679af401eda1f172402006ef8265f8bd58ea	A-LIB-LIBG-020223/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			structure - if a certificate check callback is not set, libgit2 does not perform any certificate checking. This means that by default - without configuring a certificate check callback, clients will not perform validation on the server SSH keys and may be subject to a man-in-the-middle attack. Users are encouraged to upgrade to v1.4.5 or v1.5.1. Users unable to upgrade should ensure that all relevant certificates are manually checked. **CVE ID : CVE-2023-22742**		
Affected Version(s): 1.5.0					
Improper Verification of Cryptographic Signature	20-Jan-2023	5.9	libgit2 is a cross-platform, linkable library implementation of Git. When using an SSH remote with the optional libssh2 backend, libgit2 does not perform certificate checking by default. Prior versions of libgit2 require the caller to set the `certificate_check` field of libgit2's `git_remote_callbacks` structure - if a certificate check callback is not set, libgit2 does not	https://github.com/libgit2/libgit2/commit/42e5db98b963ae503229c63e44e06e439df50e56, https://github.com/libgit2/libgit2/commit/cd6f679af401eda1f172402006ef8265f8bd58ea	A-LIB-LIBG-020223/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform any certificate checking. This means that by default - without configuring a certificate check callback, clients will not perform validation on the server SSH keys and may be subject to a man-in-the-middle attack. Users are encouraged to upgrade to v1.4.5 or v1.5.1. Users unable to upgrade should ensure that all relevant certificates are manually checked. **CVE ID : CVE-2023-22742**		
Vendor: lightftp_project					
Product: lightftp					
Affected Version(s): * Up to (including) 2.2					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21-Jan-2023	7.5	A race condition in LightFTP through 2.2 allows an attacker to achieve path traversal via a malformed FTP request. A handler thread can use an overwritten context->FileName. **CVE ID : CVE-2023-24042**	N/A	A-LIG-LIGH-020223/246
Vendor: login_with_phone_number_project					
Product: login_with_phone_number					
Affected Version(s): * Up to (excluding) 1.4.2					
Improper Neutralization of Special	20-Jan-2023	8.8	The Login with Phone Number WordPress Plugin, version < 1.4.2, is affected by an	N/A	A-LOG-LOGI-020223/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			authenticated SQL injection vulnerability in the 'ID' parameter of its 'lwp_forgot_password' action. **CVE ID : CVE-2023-23492**		
Vendor: matbao					
Product: wp_helper_premium					
Affected Version(s): * Up to (excluding) 4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2023	6.1	The WP Helper Lite WordPress plugin, in versions < 4.3, returns all GET parameters unsanitized in the response, resulting in a reflected cross-site scripting vulnerability. **CVE ID : CVE-2023-0448**	N/A	A-MAT-WP_H-020223/248
Vendor: Mediawiki					
Product: mediawiki					
Affected Version(s): * Up to (excluding) 1.35.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	5.4	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. There is XSS in Wikibase date formatting via wikibase-time-precision-* fields. This allows JavaScript execution by staff/admin users who do not intentionally	https://phabricator.wikimedia.org/T323592	A-MED-MEDI-020223/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have the editsitejs capability. **CVE ID : CVE-2023-22910**		
Use of Insufficiently Random Values	20-Jan-2023	5.3	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. CheckUser TokenManager insecurely uses AES-CTR encryption with a repeated (aka re-used) nonce, allowing an adversary to decrypt. **CVE ID : CVE-2023-22912**	https://phabricator.wikimedia.org/T315123	A-MED-MEDI-020223/250
Affected Version(s): 1.39.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	5.4	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. There is XSS in Wikibase date formatting via wikibase-time-precision-* fields. This allows JavaScript execution by staff/admin users who do not intentionally have the editsitejs capability. **CVE ID : CVE-2023-22910**	https://phabricator.wikimedia.org/T323592	A-MED-MEDI-020223/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Insufficiently Random Values	20-Jan-2023	5.3	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. CheckUser TokenManager insecurely uses AES-CTR encryption with a repeated (aka re-used) nonce, allowing an adversary to decrypt. **CVE ID : CVE-2023-22912**	https://phabricator.wikimedia.org/T315123	A-MED-MEDI-020223/252
Affected Version(s): From (including) 1.36.0 Up to (excluding) 1.38.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	5.4	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. There is XSS in Wikibase date formatting via wikibase-time-precision-* fields. This allows JavaScript execution by staff/admin users who do not intentionally have the editsitejs capability. **CVE ID : CVE-2023-22910**	https://phabricator.wikimedia.org/T323592	A-MED-MEDI-020223/253
Use of Insufficiently Random Values	20-Jan-2023	5.3	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. CheckUser	https://phabricator.wikimedia.org/T315123	A-MED-MEDI-020223/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TokenManager insecurely uses AES-CTR encryption with a repeated (aka re-used) nonce, allowing an adversary to decrypt. **CVE ID : CVE-2023-22912**		
Vendor: Microsoft					
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 108.0.1462.95					
N/A	24-Jan-2023	8.3	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability. **CVE ID : CVE-2023-21775**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21775	A-MIC-EDGE-020223/255
N/A	24-Jan-2023	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2023-21795. **CVE ID : CVE-2023-21796**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21796	A-MIC-EDGE-020223/256
Affected Version(s): * Up to (excluding) 109.0.1518.70					
N/A	24-Jan-2023	8.3	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability. **CVE ID : CVE-2023-21775**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21775	A-MIC-EDGE-020223/257
N/A	24-Jan-2023	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2023-21796.	https://portal.msrc.microsoft.com/en-US/security-guidance/advi	A-MIC-EDGE-020223/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21795	sory/CVE-2023-21795	
Incorrect Authorization	24-Jan-2023	6.5	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability. **CVE ID : CVE-2023-21719**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21719	A-MIC-EDGE-020223/259
Vendor: miniorange					
Product: ldap_integration_with_active_directory_and_openldap					
Affected Version(s): 5.0.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Jan-2023	7.5	The 'LDAP Integration with Active Directory and OpenLDAP - NTLM & Kerberos Login' extension is vulnerable to LDAP Injection since is not properly sanitizing the 'username' POST parameter. An attacker can manipulate this paramter to dump arbitrary contents form the LDAP Database. **CVE ID : CVE-2023-23749**	N/A	A-MIN-LDAP-020223/260
Vendor: Misp					
Product: misp					
Affected Version(s): 2.4.167					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	In MISP 2.4.167, app/webroot/js/action_table.js allows XSS via a network history name. **CVE ID : CVE-2023-24027**	https://github.com/MISP/MISP/commit/72c5424034c378583d128fc1e769aae33fb1c8b9	A-MIS-MISP-020223/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Misp-project					
Product: malware_information_sharing_platform					
Affected Version(s): * Up to (including) 2.4.167					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2023	6.1	app/View/AuthKeys/authkey_display.ctp in MISP through 2.4.167 has an XSS in authkey add via a Referer field. **CVE ID : CVE-2023-24070**	https://github.com/MISP/MISP/commit/f7238fe5e71ac065daa43c8607d02f8ac682f18f	A-MIS-MALW-020223/262
Product: misp					
Affected Version(s): 2.4.167					
N/A	20-Jan-2023	9.8	In MISP 2.4.167, app/Controller/Component/ACLComponent.php has incorrect access control for the decaying import function. **CVE ID : CVE-2023-24028**	https://github.com/MISP/MISP/commit/93bf15d3bd703a32ebfe86cb6c1c9b735cf23e30	A-MIS-MISP-020223/263
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jan-2023	6.1	In MISP 2.4.167, app/webroot/js/event-graph.js has an XSS vulnerability via an event-graph preview payload. **CVE ID : CVE-2023-24026**	https://github.com/MISP/MISP/commit/a46f794a136001101cbec84fccf3cc824e983493	A-MIS-MISP-020223/264
Vendor: modoboa					
Product: modoboa					
Affected Version(s): * Up to (excluding) 2.0.4					
Cross-Site Request Forgery (CSRF)	19-Jan-2023	6.5	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.0.4.	https://github.com/modoboa/modoboa/commit/8e14ac93669df4f35fcdebd55dc9	A-MOD-MODO-020223/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0398	d2f0fed3ed48, https://huntr.dev/bounties/0a852351-00ed-44d2-a650-9055b7beed58	
Cross-Site Request Forgery (CSRF)	23-Jan-2023	6.5	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.0.4. **CVE ID : CVE-2023-0438**	https://huntr.dev/bounties/07a5b61b-306d-47c4-8ff0-06c540c7dfb3, https://github.com/modoboa/modoboa/commit/38d778cc71e370216e067d054ce0169ad83078c8	A-MOD-MODO-020223/266
Cross-Site Request Forgery (CSRF)	19-Jan-2023	4.3	Cross-Site Request Forgery (CSRF) in GitHub repository modoboa/modoboa prior to 2.0.4. **CVE ID : CVE-2023-0406**	https://github.com/modoboa/modoboa/commit/7f0573e917227686d2cc127be1364e2908740807, https://huntr.dev/bounties/d7007f76-3dbc-48a7-a2fb-377040fe100c	A-MOD-MODO-020223/267
Vendor: my_youtube_channel_project					
Product: my_youtube_channel					
Affected Version(s): * Up to (including) 3.0.12.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2023	5.5	The My YouTube Channel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its settings parameters in versions up to, and including, 3.0.12.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-0446**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2844200%40youtube-channel&new=2844200%40youtube-channel&sfp_email=&sfph_mail=	A-MY_-MY_Y-020223/268
Missing Authorization	23-Jan-2023	4.3	The My YouTube Channel plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the clear_all_cache function in versions up to, and including, 3.0.12.1. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to clear the plugin's cache. **CVE ID : CVE-2023-0447**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2844200%40youtube-channel&new=2844200%40youtube-channel&sfp_email=&sfph_mail=	A-MY_-MY_Y-020223/269
Vendor: Nlnetlabs					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: krill					
Affected Version(s): * Up to (excluding) 0.12.1					
N/A	17-Jan-2023	7.5	NLnet Labs Krill supports direct access to the RRDP repository content through its built-in web server at the "/rrdp" endpoint. Prior to 0.12.1 a direct query for any existing directory under "/rrdp/", rather than an RRDP file such as "/rrdp/notification.xml " as would be expected, causes Krill to crash. If the built-in "/rrdp" endpoint is exposed directly to the internet, then malicious remote parties can cause the publication server to crash. The repository content is not affected by this, but the availability of the server and repository can cause issues if this attack is persistent and is not mitigated. **CVE ID : CVE-2023-0158**	https://www.nlnetlabs.nl/downloads/krill/CVE-2023-0158.txt	A-NLN-KRIL-020223/270
Vendor: oi_yandex.maps_project					
Product: oi_yandex.maps					
Affected Version(s): * Up to (including) 3.2.7					
Improper Neutralization of Input During Web Page Generation	23-Jan-2023	5.4	Auth. Stored Cross-Site Scripting (XSS) in Oi Yandex.Maps for WordPress <= 3.2.7 versions.	N/A	A-OI_-OI_Y-020223/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-22721**		
Vendor: online_food_ordering_system_project					
Product: online_food_ordering_system					
Affected Version(s): 2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2023	9.8	A vulnerability was found in SourceCodester Online Food Ordering System 2.0. It has been classified as critical. Affected is an unknown function of the file admin/manage_user.php. 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. The identifier of this vulnerability is VDB-218472. **CVE ID : CVE-2023-0332**	N/A	A-ONL-ONLI-020223/272
Vendor: online_tours_\&_travels_management_system_project					
Product: online_tours_\&_travels_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2023	9.8	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/page-login.php. The manipulation of the	N/A	A-ONL-ONLI-020223/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-218426 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0324**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Jan-2023	7.2	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. This issue affects some unknown processing of the file admin/forget_password.php of the component Parameter Handler. The manipulation of the argument email leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-219335. **CVE ID : CVE-2023-0515**	N/A	A-ONL-ONLI-020223/274
Improper Neutralization of Special Elements used in an SQL Command	26-Jan-2023	7.2	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been classified as critical. Affected is an unknown function of the file	N/A	A-ONL-ONLI-020223/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			user/forget_password.php of the component Parameter Handler. The manipulation of the argument email leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-219336. **CVE ID : CVE-2023-0516**		
Vendor: Oracle					
Product: access_manager					
Affected Version(s): 12.2.1.4.0					
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Access Manager executes to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Access Manager accessible data. CVSS	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-ACCE-020223/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21859**		
Product: bi_publisher					
Affected Version(s): 12.2.1.4.0					
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21832**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BI_P-020223/277
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher	https://www.oracle.com/se	A-ORA-BI_P-020223/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21846**	curity-alerts/cpujan2023.html	
Affected Version(s): 5.9.0.0.0					
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BI_P-020223/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21832**		
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BI_P-020223/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21846**		
Affected Version(s): 6.4.0.0.0					
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21832**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BI_P-020223/281
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BI_P-020223/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.9.0.0.0, 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21846**		
Product: business_intelligence					
Affected Version(s): 5.9.0.0.0					
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BUSI-020223/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21861**		
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BUSI-020223/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21891**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BUSI-020223/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21892**		
Affected Version(s): 6.4.0.0.0					
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BUSI-020223/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21861**		
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BUSI-020223/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21891**		
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Visual Analyzer). Supported versions that are affected are 5.9.0.0.0 and 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-BUSI-020223/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21892**		
Product: collaborative_planning					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Collaborative Planning product of Oracle E-Business Suite (component:	https://www.oracle.com/security-	A-ORA-COLL-020223/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Installation). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Collaborative Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Collaborative Planning accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-21858**	alerts/cpujan2023.html	
Product: communications_billing_and_revenue_management_elastic_charging_engine					
Affected Version(s): From (including) 12.0.0.3.0 Up to (including) 12.0.0.7.0					
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle Communications BRM - Elastic Charging Engine product of Oracle Communications Applications (component: Customer, Config, Pricing Manager). Supported versions that are affected are 12.0.0.3.0-12.0.0.7.0. Easily exploitable vulnerability allows	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-COMM-020223/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high privileged attacker with logon to the infrastructure where Oracle Communications BRM - Elastic Charging Engine executes to compromise Oracle Communications BRM - Elastic Charging Engine. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications BRM - Elastic Charging Engine accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21824**		
Product: communications_cloud_native_core_binding_support_function					
Affected Version(s): 22.3.0					
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle Communications BRM - Elastic Charging Engine product of Oracle Communications Applications (component: Customer, Config, Pricing Manager). Supported versions that are affected are 12.0.0.3.0-12.0.0.7.0. Easily exploitable vulnerability allows high privileged attacker with logon to the	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-COMM-020223/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			infrastructure where Oracle Communications BRM - Elastic Charging Engine executes to compromise Oracle Communications BRM - Elastic Charging Engine. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications BRM - Elastic Charging Engine accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21824**		
Product: communications_cloud_native_core_policy					
Affected Version(s): 22.3.0					
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle Communications BRM - Elastic Charging Engine product of Oracle Communications Applications (component: Customer, Config, Pricing Manager). Supported versions that are affected are 12.0.0.3.0-12.0.0.7.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Communications	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-COMM-020223/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BRM - Elastic Charging Engine executes to compromise Oracle Communications BRM - Elastic Charging Engine. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications BRM - Elastic Charging Engine accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21824**		
Product: communications_converged_application_server					
Affected Version(s): 8.0.0					
N/A	18-Jan-2023	9.8	Vulnerability in the Oracle Communications Converged Application Server product of Oracle Communications (component: Core). Supported versions that are affected are 7.1.0 and 8.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via UDP to compromise Oracle Communications Converged Application Server. Successful attacks of this vulnerability can result	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-COMM-020223/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in takeover of Oracle Communications Converged Application Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21890**		
Affected Version(s): 7.1.0					
N/A	18-Jan-2023	9.8	Vulnerability in the Oracle Communications Converged Application Server product of Oracle Communications (component: Core). Supported versions that are affected are 7.1.0 and 8.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via UDP to compromise Oracle Communications Converged Application Server. Successful attacks of this vulnerability can result in takeover of Oracle Communications Converged Application Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-COMM-020223/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21890**		
Product: communications_convergence					
Affected Version(s): 3.0.3.1.0					
N/A	18-Jan-2023	8.8	Vulnerability in the Oracle Communications Convergence product of Oracle Communications Applications (component: Admin Configuration). The supported version that is affected is 3.0.3.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Convergence. Successful attacks of this vulnerability can result in takeover of Oracle Communications Convergence. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21848**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-COMM-020223/295
Product: database					
Affected Version(s): 19c					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	6.3	Vulnerability in the Oracle Database RDBMS Security component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database RDBMS Security. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Database RDBMS Security accessible data as well as unauthorized read access to a subset of Oracle Database RDBMS Security accessible data. CVSS 3.1 Base Score 6.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:N). **CVE ID : CVE-2023-21829**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-DATA-020223/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	4.3	Vulnerability in the Oracle Database Data Redaction component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database Data Redaction. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Database Data Redaction accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21827**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-DATA-020223/297
Affected Version(s): 21c					
N/A	18-Jan-2023	6.3	Vulnerability in the Oracle Database RDBMS Security component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-DATA-020223/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with network access via Oracle Net to compromise Oracle Database RDBMS Security. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Database RDBMS Security accessible data as well as unauthorized read access to a subset of Oracle Database RDBMS Security accessible data. CVSS 3.1 Base Score 6.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:N). **CVE ID : CVE-2023-21829**		
N/A	18-Jan-2023	4.3	Vulnerability in the Oracle Database Data Redaction component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows low privileged attacker having Create Session	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-DATA-020223/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with network access via Oracle Net to compromise Oracle Database Data Redaction. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Database Data Redaction accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21827**		
Product: database_server					
Affected Version(s): 19c					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Data Provider for .NET component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TCPS to compromise Oracle Data Provider for .NET. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-DATA-020223/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Data Provider for .NET. Note: Applies also to Database client-only on Windows platform. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21893**		
Affected Version(s): 21c					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Data Provider for .NET component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TCPS to compromise Oracle Data Provider for .NET. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Data Provider for .NET. Note: Applies also to Database client-only on Windows platform. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-DATA-020223/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21893**		
Product: demantra_demand_management					
Affected Version(s): 12.1					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Demantra Demand Management product of Oracle Supply Chain (component: E-Business Collections). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Demantra Demand Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Demantra Demand Management accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-DEMA-020223/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21850		
Affected Version(s): 12.2					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Demantra Demand Management product of Oracle Supply Chain (component: E-Business Collections). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Demantra Demand Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Demantra Demand Management accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-21850**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-DEMA-020223/303
Product: e-business_suite					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Applications	https://www.oracle.com/se	A-ORA-E-BU-020223/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DBA product of Oracle E-Business Suite (component: Java utils). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications DBA. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications DBA accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-21849**	curity-alerts/cpujan2023.html	
N/A	18-Jan-2023	5.4	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: Download). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-E-BU-020223/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Web Applications Desktop Integrator, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Web Applications Desktop Integrator accessible data as well as unauthorized read access to a subset of Oracle Web Applications Desktop Integrator accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21847**		
Product: global_lifecycle_management_nextgen_oui_framework					
Affected Version(s): * Up to (excluding) 13.9.4.2.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	7.3	Vulnerability in the Oracle Global Lifecycle Management NextGen OUI Framework product of Oracle Fusion Middleware (component: NextGen Installer issues). Supported versions that are affected are Prior to 13.9.4.2.11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Global Lifecycle Management NextGen OUI Framework executes to compromise Oracle Global Lifecycle Management NextGen OUI Framework. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Global Lifecycle Management NextGen OUI Framework. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-GLOB-020223/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21894		
Product: graalvm					
Affected Version(s): 22.3.0					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g.,	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-GRAA-020223/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-GRAA-020223/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21835**		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5,	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-GRAA-020223/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Affected Version(s): 20.3.8					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-GRAA-020223/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-GRAA-020223/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21835**		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-GRAA-020223/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Affected Version(s): 21.3.4					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets,	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-GRAA-020223/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-GRAA-020223/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21835**		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-GRAA-020223/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Product: hcm_common_architecture					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle HCM Common Architecture product of Oracle E-Business Suite (component: Auomated Test Suite). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HCM Common Architecture. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HCM Common Architecture accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-21857**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-HCM_-020223/316
Product: hospitality_reporting_and_analytics					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.1.0					
N/A	18-Jan-2023	8.1	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Reporting). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21828**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-HOSP-020223/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	7.6	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Reporting). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Reporting and Analytics. CVSS 3.1 Base Score 7.6	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-HOSP-020223/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:H). **CVE ID : CVE-2023-21826**		
Product: isetup					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle iSetup product of Oracle E-Business Suite (component: General Ledger Update Transform, Reports). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSetup. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iSetup accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-21856**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-ISET-020223/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: isupplier_portal					
Affected Version(s): From (including) 12.2.6 Up to (including) 12.2.8					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle iSupplier Portal product of Oracle E-Business Suite (component: Supplier Management). Supported versions that are affected are 12.2.6-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iSupplier Portal accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21825**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-ISUP-020223/320
Product: jdk					
Affected Version(s): 1.8.0					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JDK-020223/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets,	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JDK-020223/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Affected Version(s): 11.0.17					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JDK-020223/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE).	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JDK-020223/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21835**		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JDK-020223/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Affected Version(s): 17.0.5					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JDK-020223/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JDK-020223/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21835**		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JDK-020223/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Affected Version(s): 19.0.1					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JDK-020223/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of	https://www.oracle.com/security-	A-ORA-JDK-020223/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by	alerts/cpujan 2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21835**		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JDK-020223/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Product: jre					
Affected Version(s): 1.8.0					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JRE-020223/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle	https://www.oracle.com/se	A-ORA-JRE-020223/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically	curity-alerts/cpujan2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Affected Version(s): 11.0.17					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data.	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JRE-020223/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JRE-020223/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21835**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JRE-020223/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Affected Version(s): 17.0.5					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JRE-020223/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Easily	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JRE-020223/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21835		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JRE-020223/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Affected Version(s): 19.0.1					
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8 and 21.3.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JRE-020223/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21830**		
N/A	18-Jan-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JRE-020223/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3.8, 21.3.4 and 22.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via DTLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21835		
N/A	18-Jan-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Sound). Supported versions that are affected are Oracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-JRE-020223/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21843**		
Product: learning_management					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Learning Management product of Oracle E-Business Suite (component: Setup). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Learning Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Learning Management accessible data. CVSS 3.1 Base Score 7.5 (Integrity	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-LEAR-020223/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-21852**		
Product: marketing					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-21851**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MARK-020223/344
Product: mobile_field_service					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Mobile Field Service product of Oracle E-Business Suite (component: Synchronization). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Mobile Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Mobile Field Service accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-21853**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MOBI-020223/345
Product: mysql					
Affected Version(s): From (including) 8.0 Up to (including) 8.0.31					
N/A	18-Jan-2023	5.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.31	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2023-21875**		
N/A	18-Jan-2023	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2023-21877**		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21876**		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21878**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/349
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21879**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.31					
N/A	18-Jan-2023	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2023-21880**		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21881		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21883**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/353
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21887**		
N/A	18-Jan-2023	2.7	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21882**		
Product: mysql_cluster					
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.31					
N/A	18-Jan-2023	6.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: Internal Operations). Supported versions that are affected are 7.4.38 and prior, 7.5.28 and prior, 7.6.24 and prior and 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21860**		
Affected Version(s): From (including) 7.4.0 Up to (including) 7.4.38					
N/A	18-Jan-2023	6.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: Internal Operations). Supported versions that are affected are 7.4.38 and prior, 7.5.28 and prior, 7.6.24 and prior and 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21860		
Affected Version(s): From (including) 7.5.0 Up to (including) 7.5.28					
N/A	18-Jan-2023	6.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: Internal Operations). Supported versions that are affected are 7.4.38 and prior, 7.5.28 and prior, 7.6.24 and prior and 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21860**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 7.6.0 Up to (including) 7.6.24					
N/A	18-Jan-2023	6.3	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: Internal Operations). Supported versions that are affected are 7.4.38 and prior, 7.5.28 and prior, 7.6.24 and prior and 8.0.31 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21860**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/359
Product: mysql_server					
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.31					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21868**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/360
N/A	18-Jan-2023	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2023-21869**		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21836**		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21863**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/363
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21867**		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21870**		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21871**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/366
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21873**		
Affected Version(s): From (including) 5.7.0 Up to (including) 5.7.40					
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.40 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21840**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.28					
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21866**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/369
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.29					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.29 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2023-21872**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/370
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.30					
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21864**		
N/A	18-Jan-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21865**		
N/A	18-Jan-2023	2.7	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21874**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-MYSQ-020223/373
Product: peoplesoft_enterprise_cs_academic_advisement					
Affected Version(s): 9.2					
N/A	18-Jan-2023	5.3	Vulnerability in the PeopleSoft Enterprise CS Academic	https://www.oracle.com/security-	A-ORA-PEOP-020223/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Advisement product of Oracle PeopleSoft (component: Advising Notes). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Academic Advisement. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise CS Academic Advisement accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21831**	alerts/cpujan2023.html	
Product: peoplesoft_enterprise_peopletools					
Affected Version(s): 8.59					
N/A	18-Jan-2023	5.4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows low privileged attacker with network access via	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-PEOP-020223/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21844**		
Affected Version(s): 8.60					
N/A	18-Jan-2023	5.4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-PEOP-020223/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21844**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	5.4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Panel Processor). The supported version that is affected is 8.60. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-21845**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-PEOP-020223/377
Product: primavera_gateway					
Affected Version(s): From (including) 18.8.0 Up to (including) 18.8.15					
N/A	18-Jan-2023	5.4	Vulnerability in the Primavera Gateway product of Oracle Construction and	https://www.oracle.com/security-	A-ORA-PRIM-020223/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Engineering (component: WebUI). Supported versions that are affected are 18.8.0-18.8.15, 19.12.0-19.12.15, 20.12.0-20.12.10 and 21.12.0-21.12.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Gateway. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Gateway, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Gateway accessible data as well as unauthorized read access to a subset of Primavera Gateway accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	alerts/cpujan2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21888		
Affected Version(s): From (including) 19.12.0 Up to (including) 19.12.15					
N/A	18-Jan-2023	5.4	Vulnerability in the Primavera Gateway product of Oracle Construction and Engineering (component: WebUI). Supported versions that are affected are 18.8.0-18.8.15, 19.12.0-19.12.15, 20.12.0-20.12.10 and 21.12.0-21.12.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Gateway. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Gateway, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Gateway accessible data as well as unauthorized read access to a subset of Primavera Gateway accessible data. CVSS	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-PRIM-020223/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21888**		
Affected Version(s): From (including) 20.12.0 Up to (including) 20.12.10					
N/A	18-Jan-2023	5.4	Vulnerability in the Primavera Gateway product of Oracle Construction and Engineering (component: WebUI). Supported versions that are affected are 18.8.0-18.8.15, 19.12.0-19.12.15, 20.12.0-20.12.10 and 21.12.0-21.12.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Gateway. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Gateway, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-PRIM-020223/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to some of Primavera Gateway accessible data as well as unauthorized read access to a subset of Primavera Gateway accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21888**		
Affected Version(s): From (including) 21.12.0 Up to (including) 21.12.8					
N/A	18-Jan-2023	5.4	Vulnerability in the Primavera Gateway product of Oracle Construction and Engineering (component: WebUI). Supported versions that are affected are 18.8.0-18.8.15, 19.12.0-19.12.15, 20.12.0-20.12.10 and 21.12.0-21.12.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Gateway. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Gateway, attacks may	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-PRIM-020223/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Gateway accessible data as well as unauthorized read access to a subset of Primavera Gateway accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21888**		
Product: sales_for_handhelds					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Sales for Handhelds product of Oracle E-Business Suite (component: Pocket Outlook Sync(PocketPC)). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales for Handhelds. Successful attacks of	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-SALE-020223/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sales for Handhelds accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-21855**		
Product: sales_offline					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Core Components). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales Offline. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sales Offline accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts).	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-SALE-020223/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-21854**		
Product: self-service_human_resources					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jan-2023	4.3	Vulnerability in the Oracle Self-Service Human Resources product of Oracle E-Business Suite (component: Workflow, Approval, Work Force Management). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Self-Service Human Resources. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Self-Service Human Resources accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21834**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-SELF-020223/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: vm_virtualbox					
Affected Version(s): * Up to (excluding) 6.1.42					
N/A	18-Jan-2023	8.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21886**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/385
N/A	18-Jan-2023	5.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Applies to VirtualBox VMs running Windows 7 and later. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21898**		
N/A	18-Jan-2023	5.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Applies to VirtualBox VMs running Windows 7 and later. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21899**		
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21884**		
N/A	18-Jan-2023	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: Applies to Windows only. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/P	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2023-21885**		
N/A	18-Jan-2023	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2023-21889**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/390
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	8.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21886**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/391
N/A	18-Jan-2023	5.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Applies to VirtualBox VMs running Windows 7 and later. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21898**		
N/A	18-Jan-2023	5.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: Applies to VirtualBox VMs running Windows 7 and later. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21899**		
N/A	18-Jan-2023	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts).	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21884**		
N/A	18-Jan-2023	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: Applies to Windows only. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21885		
N/A	18-Jan-2023	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.42 and prior to 7.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2023-21889**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-VM_V-020223/396
Product: weblogic_server					
Affected Version(s): 12.2.1.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21837**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/397
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21838**		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21839**		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21841**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/400
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware	https://www.oracle.com/security-	A-ORA-WEBL-020223/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21842**	alerts/cpujan2023.html	
Affected Version(s): 12.2.1.3.0					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21837**		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21838**		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21839**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/404
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21841**		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21842**		
Affected Version(s): 14.1.1.0.0					
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/P	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21837**		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21838**	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/408
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21839**		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21841**		
N/A	18-Jan-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEBL-020223/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21842		
Product: web_services_manager					
Affected Version(s): 12.2.1.4.0					
N/A	18-Jan-2023	8.1	Vulnerability in the Oracle Web Services Manager product of Oracle Fusion Middleware (component: XML Security component). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Services Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Services Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Web Services Manager accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and	https://www.oracle.com/security-alerts/cpujan2023.html	A-ORA-WEB_-020223/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21862**		
Vendor: orangescrum					
Product: orangescrum					
Affected Version(s): 2.0.11					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Jan-2023	8.8	OrangeScrum version 2.0.11 allows an authenticated external attacker to execute arbitrary commands on the server. This is possible because the application injects an attacker-controlled parameter into a system function. **CVE ID : CVE-2023-0164**	N/A	A-ORA-ORAN-020223/413
Vendor: pgadmin					
Product: pgadmin					
Affected Version(s): From (including) 4.0 Up to (excluding) 6.14					
URL Redirection to Untrusted Site ('Open Redirect')	17-Jan-2023	6.1	Open redirect vulnerability in pgAdmin 4 versions prior to v6.14 allows a remote unauthenticated attacker to redirect a user to an arbitrary web site and conduct a phishing attack by having a user to access a specially crafted URL. **CVE ID : CVE-2023-22298**	https://github.com/pgadmin-org/pgadmin4/issues/5343, https://www.pgadmin.org/	A-PGA-PGAD-020223/414
Vendor: Pimcore					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: pimcore					
Affected Version(s): * Up to (excluding) 10.5.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.14. **CVE ID : CVE-2023-0323**	https://huntr.dev/bounties/129d6a4b-0504-4de1-a72c-3f12c4552343, https://github.com/pimcore/pimcore/commit/746fac1a342841624f63ab13edcd340358e1bc04	A-PIM-PIMC-020223/415
Vendor: pkgconf					
Product: pkgconf					
Affected Version(s): * Up to (including) 1.9.3					
N/A	22-Jan-2023	9.8	In pkgconf through 1.9.3, variable duplication can cause unbounded string expansion due to incorrect checks in libpkgconf/tuple.c:pkgconf_tuple_parse. For example, a .pc file containing a few hundred bytes can expand to one billion bytes. **CVE ID : CVE-2023-24056**	https://gitea.treehouse.systems/ariadne/pkgconf/commit/628b2b2babfa5d3a2017193ddf375093e70666059	A-PKG-PKGC-020223/416
Vendor: Plesk					
Product: obsidian					
Affected Version(s): * Up to (including) 18.0.49					
URL Redirection to	22-Jan-2023	6.1	A Host Header Injection issue on the Login page of Plesk Obsidian	N/A	A-PLE-OBSI-020223/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			through 18.0.49 allows attackers to redirect users to malicious websites via a Host request header. **CVE ID : CVE-2023-24044**		
Vendor: Powerdns					
Product: recursor					
Affected Version(s): 4.8.0					
Uncontrolled Recursion	21-Jan-2023	7.5	A remote attacker might be able to cause infinite recursion in PowerDNS Recursor 4.8.0 via a DNS query that retrieves DS records for a misconfigured domain, because QName minimization is used in QM fallback mode. This is fixed in 4.8.1. **CVE ID : CVE-2023-22617**	https://docs.powerdns.com/recursor/changelog/4.8.html#change-4.8.1, https://docs.powerdns.com/recursor/security-advisories/	A-POW-RECU-020223/418
Vendor: pyload					
Product: pyload					
Affected Version(s): * Up to (including) 0.4.20					
N/A	22-Jan-2023	9.8	Excessive Attack Surface in GitHub repository pyload/pyload prior to 0.5.0b3.dev41. **CVE ID : CVE-2023-0435**	https://huntr.dev/bounties/a3e32ad5-caee-4f43-b10a-4a876d4e3f1d, https://github.com/pyload/pyload/commit/431ea6f0371d748df66	A-PYL-PYLO-020223/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				b344a05ca1a8e0310cff3	
Affected Version(s): * Up to (including) 0.4.9					
Improper Input Validation	22-Jan-2023	7.5	Improper Input Validation in GitHub repository pyload/pyload prior to 0.5.0b3.dev40. **CVE ID : CVE-2023-0434**	https://github.com/pyload/pyload/commit/a2b1eb1028f45ac58dea5f58593c1d3db2b4a104, https://huntr.dev/bounties/7d9332d8-6997-483b-9fb9-bcf2ae01dad4	A-PYL-PYLO-020223/420
Affected Version(s): 0.5.0					
Improper Input Validation	22-Jan-2023	7.5	Improper Input Validation in GitHub repository pyload/pyload prior to 0.5.0b3.dev40. **CVE ID : CVE-2023-0434**	https://github.com/pyload/pyload/commit/a2b1eb1028f45ac58dea5f58593c1d3db2b4a104, https://huntr.dev/bounties/7d9332d8-6997-483b-9fb9-bcf2ae01dad4	A-PYL-PYLO-020223/421
Vendor: Rapid7					
Product: velociraptor					
Affected Version(s): * Up to (excluding) 0.6.7-5					
Missing Authorization	18-Jan-2023	8.8	Rapid7 Velociraptor allows users to be created with different privileges on the server. Administrators are generally allowed to run any command on the server including	https://docs.velociraptor.app/announcements/2023-cves/#:~:text=to%20upgrade%20clients.-	A-RAP-VELO-020223/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			writing arbitrary files. However, lower privilege users are generally forbidden from writing or modifying files on the server. The VQL copy() function applies permission checks for reading files but does not check for permission to write files. This allows a low privilege user (usually, users with the Velociraptor "investigator" role) to overwrite files on the server, including Velociraptor configuration files. To exploit this vulnerability, the attacker must already have a Velociraptor user account at a low privilege level (at least "analyst") and be able to log into the GUI and create a notebook where they can run the VQL query invoking the copy() VQL function. Typically, most users deploy Velociraptor with limited access to a trusted group (most users will be administrators within the GUI). This vulnerability is associated with program files https://github.Com/Vel	,CVE%2D2023%2D0242,-Insufficient%20Permission%20Check	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ocidex/velociraptor/blob/master/vql/filesystem/copy.go https://github.Com/Velocidex/velociraptor/blob/master/vql/filesystem/copy.go and program routines copy(). This issue affects Velociraptor versions before 0.6.7-5. Version 0.6.7-5, released January 16, 2023, fixes the issue. **CVE ID : CVE-2023-0242**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Jan-2023	4.3	Rapid7 Velociraptor did not properly sanitize the client ID parameter to the CreateCollection API, allowing a directory traversal in where the collection task could be written. It was possible to provide a client id of "../clients/server" to schedule the collection for the server (as a server artifact), but only require privileges to schedule collections on the client. Normally, to schedule an artifact on the server, the COLLECT_SERVER permission is required. This permission is normally only granted to "administrator" role. Due to this issue, it is sufficient to have the COLLECT_CLIENT	N/A	A-RAP-VELO-020223/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege, which is normally granted to the "investigator" role. To exploit this vulnerability, the attacker must already have a Velociraptor user account at least "investigator" level, and be able to authenticate to the GUI and issue an API call to the backend. Typically, most users deploy Velociraptor with limited access to a trusted group, and most users will already be administrators within the GUI. This issue affects Velociraptor versions before 0.6.7-5. Version 0.6.7-5, released January 16, 2023, fixes the issue. **CVE ID : CVE-2023-0290**		
Vendor: Redhat					
Product: openshift					
Affected Version(s): 4.11					
Use of a Broken or Risky Cryptographic Algorithm	17-Jan-2023	5.3	The Birthday attack against 64-bit block ciphers flaw (CVE-2016-2183) was reported for the health checks port (9979) on etcd grpc-proxy component. Even though the CVE-2016-2183 has been fixed in the etcd components, to enable periodic health checks from kubelet, it	N/A	A-RED-OPEN-020223/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was necessary to open up a new port (9979) on etcd grpc-proxy, hence this port might be considered as still vulnerable to the same type of vulnerability. The health checks on etcd grpc-proxy do not contain sensitive data (only metrics data), therefore the potential impact related to this vulnerability is minimal. The CVE-2023-0296 has been assigned to this issue to track the permanent fix in the etcd component. **CVE ID : CVE-2023-0296**		
Vendor: rockstargames					
Product: grand_theft_auto_v					
Affected Version(s): -					
N/A	22-Jan-2023	7.3	Grand Theft Auto V for PC allows attackers to achieve partial remote code execution or modify files on a PC, as exploited in the wild in January 2023. **CVE ID : CVE-2023-24059**	https://support.rockstargames.com/community/2000 63373/13252 523900819, https://support.rockstargames.com/community/2000 63373/13249 062368147	A-ROC-GRAN-020223/425
Vendor: sandhillsdev					
Product: easy_digital_downloads					
Affected Version(s): * Up to (excluding) 3.1.0.4					
Improper Neutralizat	20-Jan-2023	9.8	The Easy Digital Downloads WordPress	N/A	A-SAN-EASY-020223/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Plugin, version < 3.1.0.4, is affected by an unauthenticated SQL injection vulnerability in the 's' parameter of its 'edd_download_search' action. **CVE ID : CVE-2023-23489**		
Vendor: Shopware					
Product: shopware					
Affected Version(s): * Up to (excluding) 6.4.18.1					
Insufficient Session Expiration	17-Jan-2023	9.8	Shopware is an open source commerce platform based on Symfony Framework and Vue js. The Administration session expiration was set to one week, when an attacker has stolen the session cookie they could use it for a long period of time. In version 6.4.18.1 an automatic logout into the Administration session has been added. As a result the user will be logged out when they are inactive. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-22732**	https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-01-2023?category=security-updates, https://github.com/shopware/platform/commit/cd7a89cbcd3a0428c6d1ef27b3aa15467a722ff6	A-SHO-SHOP-020223/427
Improper Control of Generation of Code	17-Jan-2023	8.8	Shopware is an open source commerce platform based on Symfony Framework	https://docs.shopware.com/en/shopware-6-	A-SHO-SHOP-020223/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			and Vue js. In a Twig environment **without the Sandbox extension**, it is possible to refer to PHP functions in twig filters like `map`, `filter`, `sort`. This allows a template to call any global PHP function and thus execute arbitrary code. The attacker must have access to a Twig environment in order to exploit this vulnerability. This problem has been fixed with 6.4.18.1 with an override of the specified filters until the integration of the Sandbox extension has been finished. Users are advised to upgrade. Users of major versions 6.1, 6.2, and 6.3 may also receive this fix via a plugin. **CVE ID : CVE-2023-22731**	en/security-updates/security-update-01-2023?category=security-updates, https://github.com/shopware/platform/commit/89d1ea154689cb6202e0d3a0ceeae0febb0c09e1	
Improper Input Validation	17-Jan-2023	7.5	Shopware is an open source commerce platform based on Symfony Framework and Vue js. In affected versions It was possible to put the same line item multiple times in the cart using the AP. The Cart Validators checked the line item's individuality and the user was able to bypass	https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-01-2023?category=security-updates, https://github.com/shopw	A-SHO-SHOP-020223/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			quantity limits in sales. This problem has been fixed with version 6.4.18.1. Users on major versions 6.1, 6.2, and 6.3 may also obtain this fix via a plugin. **CVE ID : CVE-2023-22730**	are/platform/commit/4fce12096e54b2033832d9104fa2e68888c2b4e9	
Improper Input Validation	17-Jan-2023	7.5	Shopware is an open source commerce platform based on Symfony Framework and Vue js. The newsletter double opt-in validation was not checked properly, and it was possible to skip the complete double opt in process. As a result operators may have inconsistencies in their newsletter systems. This problem has been fixed with version 6.4.18.1. Users are advised to upgrade. Users unable to upgrade may find security measures are available via a plugin for major versions 6.1, 6.2, and 6.3. Users may also disable newsletter registration completely. **CVE ID : CVE-2023-22734**	https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-01-2023?category=security-updates, https://github.com/shopware/platform/commit/f5a95ee2bcf1e546878450963ef1d9886e59a620	A-SHO-SHOP-020223/430
Insertion of Sensitive Information into Log File	17-Jan-2023	6.5	Shopware is an open source commerce platform based on Symfony Framework and Vue js. In affected versions the log module	https://github.com/shopware/platform/commit/407a83063d7141c1a626441799	A-SHO-SHOP-020223/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would write out all kind of sent mails. An attacker with access to either the local system logs or a centralized logging store may have access to other users accounts. This issue has been addressed in version 6.4.18.1. For older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version. Users unable to upgrade may remove from all users the log module ACL rights or disable logging. **CVE ID : CVE-2023-22733**	c3ebef79498c07, https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-01-2023?category=security-updates	
Vendor: signalwire					
Product: sofia-sip					
Affected Version(s): * Up to (excluding) 1.13.11					
Out-of-bounds Write	19-Jan-2023	9.8	Sofia-SIP is an open-source SIP User-Agent library, compliant with the IETF RFC3261 specification. In affected versions Sofia-SIP **lacks both message length and attributes length checks** when it handles STUN packets, leading to controllable heap-over-flow. For	https://github.com/freeswitch/sofia-sip/commit/da53e4fbcb138b080a75576dd49c1fff2ada2764, https://github.com/freeswitch/sofia-sip/security/advisories/GH	A-SIG-SOFI-020223/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example, in stun_parse_attribute(), after we get the attribute's type and length value, the length will be used directly to copy from the heap, regardless of the message's left size. Since network users control the overflowed length, and the data is written to heap chunks later, attackers may achieve remote code execution by heap grooming or other exploitation methods. The bug was introduced 16 years ago in sofia-sip 1.12.4 (plus some patches through 12/21/2006) to in tree libs with git-svn-id: http://svn.freeswitch.org/svn/freeswitch/trunk@3774 d0543943-73ff-0310-b7d9-9358b9ac24b2. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-22741**	SA-8599-x7rq-fr54	
Vendor: strangerstudios					
Product: paid_memberships_pro					
Affected Version(s): * Up to (excluding) 2.9.8					
Improper Neutralization of Special	20-Jan-2023	9.8	The Paid Memberships Pro WordPress Plugin, version < 2.9.8, is affected by an	N/A	A-STR-PAID-020223/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			unauthenticated SQL injection vulnerability in the 'code' parameter of the '/pmpro/v1/order' REST route. **CVE ID : CVE-2023-23488**		
Vendor: sudo_project					
Product: sudo					
Affected Version(s): 1.9.12					
Improper Privilege Management	18-Jan-2023	7.8	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists because a user-specified editor may contain a "--" argument that defeats a protection mechanism, e.g., an EDITOR='vim -- /path/to/extra/file' value. **CVE ID : CVE-2023-22809**	https://www.sudo.ws/security/advisories/sudoedit_any/, https://security.netapp.com/advisory/ntap-20230127-0015/	A-SUD-SUDO-020223/434
Affected Version(s): From (including) 1.8.0 Up to (excluding) 1.9.12					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	18-Jan-2023	7.8	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists because a user-specified editor may contain a "--" argument that defeats a protection mechanism, e.g., an EDITOR='vim --/path/to/extra/file' value. **CVE ID : CVE-2023-22809**	https://www.sudo.ws/security/advisories/sudoedit_any/, https://security.netapp.com/advisory/ntap-20230127-0015/	A-SUD-SUDO-020223/435
Vendor: Tenable					
Product: nessus					
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.4.2					
Improper Privilege Management	20-Jan-2023	8.8	A privilege escalation vulnerability was identified in Nessus versions 8.10.1 through 8.15.8 and 10.0.0 through 10.4.1. An authenticated attacker could potentially execute a specially crafted file to obtain root or NT AUTHORITY	https://www.tenable.com/security/tns-2023-02, https://www.tenable.com/security/tns-2023-01	A-TEN-NESS-020223/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/ SYSTEM privileges on the Nessus host. **CVE ID : CVE-2023-0101**		
Affected Version(s): From (including) 8.10.1 Up to (excluding) 8.15.8					
Improper Privilege Management	20-Jan-2023	8.8	A privilege escalation vulnerability was identified in Nessus versions 8.10.1 through 8.15.8 and 10.0.0 through 10.4.1. An authenticated attacker could potentially execute a specially crafted file to obtain root or NT AUTHORITY / SYSTEM privileges on the Nessus host. **CVE ID : CVE-2023-0101**	https://www.tenable.com/security/tns-2023-02, https://www.tenable.com/security/tns-2023-01	A-TEN-NESS-020223/437
Vendor: theradsystem_project					
Product: theradsystem					
Affected Version(s): * Up to (excluding) 2015-04-03					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2023	6.1	A vulnerability was found in saemorris TheRadSystem. It has been classified as problematic. Affected is an unknown function of the file users.php. The manipulation of the argument q leads to cross site scripting. It is possible to launch the attack remotely. VDB-218454 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-0327**	https://github.com/saemorris/TheRadSystem/commit/bfba26bd34af31648a11af35a0bb66f1948752a6	A-THE-THER-020223/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: tpm2_software_stack_project					
Product: tpm2_software_stack					
Affected Version(s): * Up to (including) 4.0.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Jan-2023	6.4	tpm2-tss is an open source software implementation of the Trusted Computing Group (TCG) Trusted Platform Module (TPM) 2 Software Stack (TSS2). In affected versions `Tss2_RC_SetHandler` and `Tss2_RC_Decode` both index into `layer_handler` with an 8 bit layer number, but the array only has `TPM2_ERROR_TSS2_RC_LAYER_COUNT` entries, so trying to add a handler for higher-numbered layers or decode a response code with such a layer number reads/writes past the end of the buffer. This Buffer overrun, could result in arbitrary code execution. An example attack would be a MiTM bus attack that returns 0xFFFFFFFF for the RC. Given the common use case of TPM modules an attacker must have local access to the target machine with local system privileges which allows access to the TPM system. Usually TPM access	https://github.com/tpm2-software/tpm2-tss/commit/306490c8d848c367faa2d9df81f5e69dab46ffb5	A-TPM-TPM2-020223/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requires administrative privilege. **CVE ID : CVE-2023-22745**		
Vendor: trellix					
Product: skyhigh_secure_web_gateway					
Affected Version(s): 12.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	6.1	A cross-site scripting vulnerability in Skyhigh SWG in main releases 11.x prior to 11.2.6, 10.x prior to 10.2.17, and controlled release 12.x prior to 12.0.1 allows a remote attacker to craft SWG-specific internal requests with URL paths to any third-party website, causing arbitrary content to be injected into the response when accessed through SWG. **CVE ID : CVE-2023-0214**	https://kcm.trellix.com/corporate/index?page=content&id=SB10393	A-TRE-SKYH-020223/440
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.2.17					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	6.1	A cross-site scripting vulnerability in Skyhigh SWG in main releases 11.x prior to 11.2.6, 10.x prior to 10.2.17, and controlled release 12.x prior to 12.0.1 allows a remote attacker to craft SWG-specific internal requests with URL paths to any third-party website, causing arbitrary content to be	https://kcm.trellix.com/corporate/index?page=content&id=SB10393	A-TRE-SKYH-020223/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected into the response when accessed through SWG. **CVE ID : CVE-2023-0214**		
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	6.1	A cross-site scripting vulnerability in Skyhigh SWG in main releases 11.x prior to 11.2.6, 10.x prior to 10.2.17, and controlled release 12.x prior to 12.0.1 allows a remote attacker to craft SWG-specific internal requests with URL paths to any third-party website, causing arbitrary content to be injected into the response when accessed through SWG. **CVE ID : CVE-2023-0214**	https://kcm.trellix.com/corporate/index?page=content&id=SB10393	A-TRE-SKYH-020223/442
Vendor: Trustwave					
Product: modsecurity					
Affected Version(s): * Up to (excluding) 2.9.7					
N/A	20-Jan-2023	9.8	Incorrect handling of '\0' bytes in file uploads in ModSecurity before 2.9.7 may allow for Web Application Firewall bypasses and buffer overflows on the Web Application Firewall when executing rules that read the FILES_TMP_CONTENT collection.	https://github.com/SpiderLabs/ModSecurity/pull/2857/commits/4324f0ac59f8225aa44bc5034df60dbeccd1d334, https://github.com/SpiderLabs/ModSec	A-TRU-MODS-020223/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24021	urity/pull/2857	
Vendor: twinkletoessoftware					
Product: booked					
Affected Version(s): 2.5.5					
N/A	22-Jan-2023	4.3	Booked Scheduler 2.5.5 allows authenticated users to create and schedule events for any other user via a modified userId value to reservation_save.php. NOTE: 2.5.5 is a version from 2014; the latest version of Booked Scheduler is not affected. However, LabArchives Scheduler (Sep 6, 2022 Feature Release) is affected. **CVE ID : CVE-2023-24058**	https://www.labarchives.com/labarchives-knowledge-base/2022-feature-releases-2/, https://www.bookedscheduler.com/the-future-of-booked/	A-TWI-BOOK-020223/444
Vendor: unistra					
Product: impatient					
Affected Version(s): * Up to (excluding) 1.5.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	7.6	IMPatienT before 1.5.2 allows stored XSS via onmouseover in certain text fields within a PATCH /modify_onto request to the ontology builder. This may allow attackers to steal Protected Health Information. **CVE ID : CVE-2023-23637**	https://github.com/lambda-science/IMPatienT/issues/101, https://github.com/lambda-science/IMPatienT/compare/v1.5.1...v1.5.2, https://github.com/lambd	A-UNI-IMPA-020223/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				a-science/IMPatienT/releases/tag/v1.5.2	
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.0.1225					
Heap-based Buffer Overflow	21-Jan-2023	7.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1225. **CVE ID : CVE-2023-0433**	https://github.com/vim/vim/commit/11977f917506d950b7e0cae558bd9189260b253b, https://huntr.dev/bounties/ae933869-a1ec-402a-bbea-d51764c6618e	A-VIM-VIM-020223/446
Vendor: warfareplugins					
Product: social_warfare					
Affected Version(s): * Up to (excluding) 4.4.0					
Cross-Site Request Forgery (CSRF)	19-Jan-2023	5.4	The Social Warfare plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.4.0. This is due to missing or incorrect nonce validation on several AJAX actions. This makes it possible for unauthenticated attackers to delete post meta information and reset network access tokens, via forged request granted they	N/A	A-WAR-SOCI-020223/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-0403**		
Affected Version(s): * Up to (including) 4.3.0					
Missing Authorization	19-Jan-2023	5.4	The Social Warfare plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on several AJAX actions in versions up to, and including, 4.3.0. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete post meta information and reset network access tokens. **CVE ID : CVE-2023-0402**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2844092%40social-warfare&new=2844092%40social-warfare&sfp_email=&sfph_mail=	A-WAR-SOCI-020223/448
Vendor: Wireshark					
Product: wireshark					
Affected Version(s): From (including) 3.6.0 Up to (including) 3.6.10					
Excessive Iteration	26-Jan-2023	6.5	Excessive loops in multiple dissectors in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0411**	https://www.wireshark.org/security/wnpa-sec-2023-06.html, https://gitlab.com/wireshark/wireshark/-/issues/18737, https://gitlab.	A-WIR-WIRE-020223/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				com/wireshark/wireshark/-/issues/18711, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0411.json	
Improper Resource Shutdown or Release	26-Jan-2023	6.5	TIPC dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0412**	https://gitlab.com/wireshark/wireshark/-/issues/18770, https://www.wireshark.org/security/wnpa-sec-2023-07.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0412.json	A-WIR-WIRE-020223/450
Improper Resource Shutdown or Release	26-Jan-2023	6.5	Dissection engine bug in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0413**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0413.json, https://www.wireshark.org/security/wnpa-sec-2023-03.html, https://gitlab.	A-WIR-WIRE-020223/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				com/wireshark/wireshark/-/issues/18766	
Improper Resource Shutdown or Release	26-Jan-2023	6.5	iSCSI dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0415**	https://gitlab.com/wireshark/wireshark/-/issues/18796, https://www.wireshark.org/security/wnpa-sec-2023-05.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0415.json	A-WIR-WIRE-020223/452
Improper Resource Shutdown or Release	26-Jan-2023	6.5	GNW dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0416**	https://gitlab.com/wireshark/wireshark/-/issues/18779, https://www.wireshark.org/security/wnpa-sec-2023-04.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0416.json	A-WIR-WIRE-020223/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	26-Jan-2023	6.5	Memory leak in the NFS dissector in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0417**	https://www.wireshark.org/security/wnpa-sec-2023-02.html, https://gitlab.com/wireshark/wireshark/-/issues/18628, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0417.json	A-WIR-WIRE-020223/454
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.2					
Excessive Iteration	26-Jan-2023	6.5	Excessive loops in multiple dissectors in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0411**	https://www.wireshark.org/security/wnpa-sec-2023-06.html, https://gitlab.com/wireshark/wireshark/-/issues/18737, https://gitlab.com/wireshark/wireshark/-/issues/18711, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0411.json	A-WIR-WIRE-020223/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	26-Jan-2023	6.5	TIPC dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0412**	https://gitlab.com/wireshark/wireshark/-/issues/18770, https://www.wireshark.org/security/wnpa-sec-2023-07.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0412.json	A-WIR-WIRE-020223/456
Improper Resource Shutdown or Release	26-Jan-2023	6.5	Dissection engine bug in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0413**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0413.json, https://www.wireshark.org/security/wnpa-sec-2023-03.html, https://gitlab.com/wireshark/wireshark/-/issues/18766	A-WIR-WIRE-020223/457
Improper Resource Shutdown or Release	26-Jan-2023	6.5	Crash in the EAP dissector in Wireshark 4.0.0 to 4.0.2 allows denial of service via packet injection or crafted capture file	https://www.wireshark.org/security/wnpa-sec-2023-01.html, https://gitlab.com/gitlab-	A-WIR-WIRE-020223/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0414	org/cves/-/blob/master/2023/CVE-2023-0414.json, https://gitlab.com/wireshark/wireshark/-/issues/18622	
Improper Resource Shutdown or Release	26-Jan-2023	6.5	iSCSI dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0415**	https://gitlab.com/wireshark/wireshark/-/issues/18796, https://www.wireshark.org/security/wnpa-sec-2023-05.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0415.json	A-WIR-WIRE-020223/459
Improper Resource Shutdown or Release	26-Jan-2023	6.5	GNW dissector crash in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0416**	https://gitlab.com/wireshark/wireshark/-/issues/18779, https://www.wireshark.org/security/wnpa-sec-2023-04.html, https://gitlab.com/gitlab-org/cves/-	A-WIR-WIRE-020223/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				/blob/master/2023/CVE-2023-0416.json	
Improper Resource Shutdown or Release	26-Jan-2023	6.5	Memory leak in the NFS dissector in Wireshark 4.0.0 to 4.0.2 and 3.6.0 to 3.6.10 and allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-0417**	https://www.wireshark.org/security/wnpa-sec-2023-02.html, https://gitlab.com/wireshark/wireshark/-/issues/18628, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0417.json	A-WIR-WIRE-020223/461
Vendor: wp_topbar_project					
Product: wp_topbar					
Affected Version(s): * Up to (including) 5.36					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jan-2023	8.8	Auth. SQL Injection (SQLi) vulnerability in WP-TopBar <= 5.36 versions. **CVE ID : CVE-2023-23824**	N/A	A-WP_-WP_T-020223/462
Vendor: youtube_shortcode_project					
Product: youtube_shortcode					
Affected Version(s): * Up to (including) 1.8.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2023	5.4	Auth. Stored Cross-Site Scripting (XSS) vulnerability in Youtube shortcode <= 1.8.5 versions. **CVE ID : CVE-2023-23687**	N/A	A-YOU-YOUT-020223/463
Vendor: zdir_project					
Product: zdir					
Affected Version(s): 3.2.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jan-2023	8.8	An arbitrary file upload vulnerability in the /api/upload component of zdir v3.2.0 allows attackers to execute arbitrary code via a crafted .ssh file. **CVE ID : CVE-2023-23314**	https://github.com/helloxz/zdir/issues/90	A-ZDI-ZDIR-020223/464
Vendor: Zohocorp					
Product: manageengine_exchange_reporter_plus					
Affected Version(s): * Up to (excluding) 5.7					
Improper Restriction of XML External Entity Reference	17-Jan-2023	7.5	Zoho ManageEngine Exchange Reporter Plus before 5708 allows attackers to conduct XXE attacks. **CVE ID : CVE-2023-22624**	https://www.manageengine.com/products/exchange-reports/advisory/CVE-2023-22624.html	A-ZOH-MANA-020223/465
Affected Version(s): 5.7					
Improper Restriction of XML External Entity Reference	17-Jan-2023	7.5	Zoho ManageEngine Exchange Reporter Plus before 5708 allows attackers to conduct XXE attacks.	https://www.manageengine.com/products/exchange-reports/advisory/CVE-	A-ZOH-MANA-020223/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22624	2023-22624.html	
Product: manageengine_servicedesk_plus_msp					
Affected Version(s): 10.6					
Improper Authentication	20-Jan-2023	9.1	Zoho ManageEngine ServiceDesk Plus MSP before 10611, and 13x before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled. **CVE ID : CVE-2023-22964**	https://www.manageengine.com/products/service-desk-msp/cve-2023-22964.html	A-ZOH-MANA-020223/467
Affected Version(s): 13.0					
Improper Authentication	20-Jan-2023	9.1	Zoho ManageEngine ServiceDesk Plus MSP before 10611, and 13x before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled. **CVE ID : CVE-2023-22964**	https://www.manageengine.com/products/service-desk-msp/cve-2023-22964.html	A-ZOH-MANA-020223/468
Hardware					
Vendor: ate-mahoroba					
Product: maho-pbx_netdevancer					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated attacker to execute an arbitrary OS command. **CVE ID : CVE-2023-22279**		
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	Cross-site request forgery (CSRF) vulnerability in MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. **CVE ID : CVE-2023-22286**	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/470
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-22280**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22296**	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/472
Product: maho-pbx_netdevancer_mobilegate					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver.1.11.00 allow a remote unauthenticated attacker to execute an arbitrary OS command. **CVE ID : CVE-2023-22279**		
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	Cross-site request forgery (CSRF) vulnerability in MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. **CVE ID : CVE-2023-22286**	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/474
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-22280**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22296**	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/476
Product: maho-pbx_netdevancer_vsg					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute an arbitrary OS command. **CVE ID : CVE-2023-22279**		
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	Cross-site request forgery (CSRF) vulnerability in MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. **CVE ID : CVE-2023-22286**	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/478
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. **CVE ID : CVE-2023-22280**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22296**	https://www.ate-mahoroba.jp/netdevancer/manual/	H-ATE-MAHO-020223/480
Vendor: Cisco					
Product: email_security_appliance_c160					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	H-CIS-EMAI-020223/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**		
Product: email_security_appliance_c170					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	H-CIS-EMAI-020223/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**		
Product: email_security_appliance_c190					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	H-CIS-EMAI-020223/483
Product: email_security_appliance_c370					
Affected Version(s): -					
Improper Neutralization of Special	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for	https://sec.cloudapps.cisco.com/security/center/conte	H-CIS-EMAI-020223/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**	nt/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	
Product: email_security_appliance_c370d					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	H-CIS-EMAI-020223/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**		
Product: email_security_appliance_c380					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	H-CIS-EMAI-020223/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20057		
Product: email_security_appliance_c390					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	H-CIS-EMAI-020223/487
Product: email_security_appliance_c670					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-	H-CIS-EMAI-020223/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**	url-bypass-WbMQqNJh	
Product: email_security_appliance_c680					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	H-CIS-EMAI-020223/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**		
Product: email_security_appliance_c690					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	H-CIS-EMAI-020223/490
Product: email_security_appliance_c690x					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	H-CIS-EMAI-020223/491
Product: email_security_appliance_x1070					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Componen	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	H-CIS-EMAI-020223/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t ('Injection')			reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**		
Product: ip_phones_8832					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_7800					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/494
Product: ip_phone_7811					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface	https://sec.cloudapps.cisco.com/security	H-CIS-IP_P-020223/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	
Product: ip_phone_7821					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_7832					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ip_phone_7841					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/498
Product: ip_phone_7861					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_8800					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_8811					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/501
Product: ip_phone_8821					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800	https://sec.cloudapps.cisco.com/security/center/conte	H-CIS-IP_P-020223/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	nt/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	
Product: ip_phone_8821-ex					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_8831					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/504
Product: ip_phone_8832					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/505
Product: ip_phone_8841					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_8845					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_8851					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/508
Product: ip_phone_8861					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	H-CIS-IP_P-020223/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	ityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	
Product: ip_phone_8865					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-IP_P-020223/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: rv016					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. **CVE ID : CVE-2023-20025**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	H-CIS-RV01-020223/511
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business	https://sec.cloudapps.cisco.com/security/center/conte	H-CIS-RV01-020223/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. **CVE ID : CVE-2023-20026**	nt/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	
Product: rv042					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-	H-CIS-RV04-020223/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. **CVE ID : CVE-2023-20025**	vuln-ej76Pke5	
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	H-CIS-RV04-020223/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. **CVE ID : CVE-2023-20026**		
Product: rv042g					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. **CVE ID : CVE-2023-20025**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	H-CIS-RV04-020223/515
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	H-CIS-RV04-020223/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. **CVE ID : CVE-2023-20026**	sco-sa-sbr042-multi-vuln-ej76Pke5	
Product: rv082					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	H-CIS-RV08-020223/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. **CVE ID : CVE-2023-20025**		
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	H-CIS-RV08-020223/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have valid Administrator credentials on the affected device. **CVE ID : CVE-2023-20026**		
Product: rv160w_wireless-ac_vpn_router					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-cmd-exe-n47kJQLE	H-CIS-RV16-020223/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			level credentials on the affected device. **CVE ID : CVE-2023-20045**		
Product: rv160_vpn_router					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator-level credentials on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-cmd-exe-n47kJQLE	H-CIS-RV16-020223/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20045		
Product: rv260p_vpn_router_with_poe					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator-level credentials on the affected device. **CVE ID : CVE-2023-20045**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-cmd-exe-n47kJQLE	H-CIS-RV26-020223/521
Product: rv260_vpn_router					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator-level credentials on the affected device. **CVE ID : CVE-2023-20045**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-cmd-exe-n47kJQLE	H-CIS-RV26-020223/522
Product: rv340					
Affected Version(s): -					
Improper Neutralizat	20-Jan-2023	7.2	A vulnerability in the web-based	https://sec.cloudapps.cisco	H-CIS-RV34-020223/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. **CVE ID : CVE-2023-20007**	.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD	
Product: rv340w					
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')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. **CVE ID : CVE-2023-20007**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD	H-CIS-RV34-020223/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rv345					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD	H-CIS-RV34-020223/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20007		
Product: rv345p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD	H-CIS-RV34-020223/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restart, resulting in a DoS condition. **CVE ID : CVE-2023-20007**		
Product: unified_ip_phone_8851nr					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-UNIF-020223/527
Product: unified_ip_phone_8865nr					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	H-CIS-UNIF-020223/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	ityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	
Product: webex_room_phone					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	20-Jan-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lldp-memlk-McOecPT	H-CIS-WEBE-020223/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. **CVE ID : CVE-2023-20047**		
Product: webex_share					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	20-Jan-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lldp-memlk-McOecPT	H-CIS-WEBE-020223/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. **CVE ID : CVE-2023-20047**		
Product: wireless_ip_phone_8821					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-WIRE-020223/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: wireless_ip_phone_8821-ex					
Affected Version(s): -					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	H-CIS-WIRE-020223/532
Vendor: Dell					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: powervault_me5012					
Affected Version(s): -					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. **CVE ID : CVE-2023-23691**	https://www.dell.com/support/kbdoc/en-us/000207533/dsa-2023-018-dell-emc-powervault-me5-security-update-for-a-client-desync-attack-vulnerability	H-DEL-POWE-020223/533
Product: powervault_me5024					
Affected Version(s): -					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. **CVE ID : CVE-2023-23691**	https://www.dell.com/support/kbdoc/en-us/000207533/dsa-2023-018-dell-emc-powervault-me5-security-update-for-a-client-desync-attack-vulnerability	H-DEL-POWE-020223/534
Product: powervault_me5084					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. **CVE ID : CVE-2023-23691**	https://www.dell.com/support/kbdoc/en-us/000207533/dsa-2023-018-dell-emc-powervault-me5-security-update-for-a-client-desync-attack-vulnerability	H-DEL-POWE-020223/535
Vendor: Omron					
Product: cp1l-el20dr-d					
Affected Version(s): -					
N/A	17-Jan-2023	9.8	Active debug code exists in OMRON CP1L-EL20DR-D all versions, which may lead to a command that is not specified in FINS protocol being executed without authentication. A remote unauthenticated attacker may read/write in arbitrary area of the device memory, which may lead to overwriting the firmware, causing a denial-of-service (DoS) condition, and/or arbitrary code execution. **CVE ID : CVE-2023-22357**	N/A	H-OMR-CP1L-020223/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cx-motion-mch					
Affected Version(s): -					
Access of Uninitialized Pointer	17-Jan-2023	7.8	CX-Motion-MCH v2.32 and earlier contains an access of uninitialized pointer vulnerability. Having a user to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution. **CVE ID : CVE-2023-22366**	N/A	H-OMR-CX-M-020223/537
Vendor: pixela					
Product: pix-rt100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	8	OS command injection vulnerability in PIX-RT100 versions RT100_TEQ_2.1.1_EQ101 and RT100_TEQ_2.1.2_EQ101 allows a network-adjacent attacker who can access product settings to execute an arbitrary OS command. **CVE ID : CVE-2023-22304**	https://www.pixela.co.jp/products/network/pix_rt100/update.html	H-PIX-PIX--020223/538
N/A	17-Jan-2023	6.5	Hidden functionality vulnerability in PIX-RT100 versions RT100_TEQ_2.1.1_EQ101 and RT100_TEQ_2.1.2_EQ101 allows a network-adjacent attacker to access the product via undocumented Telnet or SSH services.	https://www.pixela.co.jp/products/network/pix_rt100/update.html	H-PIX-PIX--020223/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22316		
Vendor: Sonicwall					
Product: sma1000					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Jan-2023	7.5	Pre-authentication path traversal vulnerability in SMA1000 firmware version 12.4.2, which allows an unauthenticated attacker to access arbitrary files and directories stored outside the web root directory. **CVE ID : CVE-2023-0126**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0001	H-SON-SMA1-020223/540
Vendor: Tenda					
Product: ac18					
Affected Version(s): -					
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/FUN_000c2318. **CVE ID : CVE-2023-24164**	N/A	H-TEN-AC18-020223/541
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/initIpAddrInfo. **CVE ID : CVE-2023-24165**	N/A	H-TEN-AC18-020223/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/formWifiBasicSet. **CVE ID : CVE-2023-24166**	N/A	H-TEN-AC18-020223/543
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/add_white_node. **CVE ID : CVE-2023-24167**	N/A	H-TEN-AC18-020223/544
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/FUN_0007343c. **CVE ID : CVE-2023-24169**	N/A	H-TEN-AC18-020223/545
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/fromSetWirelessRepeat. **CVE ID : CVE-2023-24170**	N/A	H-TEN-AC18-020223/546
Vendor: Tp-link					
Product: tl-sg105pe					
Affected Version(s): 1.0					
Improper Authentication	17-Jan-2023	9.8	TP-Link SG105PE firmware prior to 'TL-SG105PE(UN) 1.0_1.0.0 Build 20221208' contains an	https://www.tp-link.com/jp/support/download/tl-	H-TP--TL-S-020223/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication bypass vulnerability. Under the certain conditions, an attacker may impersonate an administrator of the product. As a result, information may be obtained and/or the product's settings may be altered with the privilege of the administrator. **CVE ID : CVE-2023-22303**	sg105pe/v1/#Firmware, https://www.tp-link.com/en/business-networking/easy-smart-switch/tl-sg105pe/	
Vendor: Trendnet					
Product: tew-820ap					
Affected Version(s): 1.0r					
Out-of-bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formSystemCheck. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-24095**	N/A	H-TRE-TEW--020223/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the newpass parameter at /formPasswordSetup. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-24096**	N/A	H-TRE-TEW--020223/549
Out-of-bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formPasswordAuth. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-24097**	N/A	H-TRE-TEW--020223/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formSysLog. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-24098**	N/A	H-TRE-TEW--020223/551
Out-of-bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the username parameter at /formWizardPassword. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-24099**	N/A	H-TRE-TEW--020223/552
Operating System					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Integer Overflow or Wraparound	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound 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-2023-21579**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/553
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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.	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21604		
Heap-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21605**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/555
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21606**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21607**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/557
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21608**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/558
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx.adobe.com/security/produc	O-APP-MACO-030223/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30418 (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-2023-21609**	ts/acrobat/apsb23-01.html	
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21610**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/560
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21611**		
Creation of Temporary File in Directory with Insecure Permissions	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21612**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/562
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-21581**		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21585**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/564
Use After Free	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage	https://helpx.adobe.com/security/products/dimension/apsb23-10.html	O-APP-MACO-030223/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-21601**		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-21603**	https://helpx.adobe.com/security/products/dimension/apsb23-10.html	O-APP-MACO-030223/566
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-21613**		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21614**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-APP-MACO-030223/568
Vendor: ate-mahoroba					
Product: maho-pbx_netdevancer_firmware					
Affected Version(s): * Up to (excluding) 1.11.00					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute an arbitrary OS command. **CVE ID : CVE-2023-22279**		
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	Cross-site request forgery (CSRF) vulnerability in MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. **CVE ID : CVE-2023-22286**	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/570
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute an arbitrary OS command. **CVE ID : CVE-2023-22280**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22296**	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/572
Product: maho-pbx_netdevancer_mobilegate_firmware					
Affected Version(s): * Up to (excluding) 1.11.00					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated attacker to execute an arbitrary OS command.	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22279		
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	Cross-site request forgery (CSRF) vulnerability in MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. **CVE ID : CVE-2023-22286**	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/574
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command.	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22280		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22296**	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/576
Product: maho-pbx_netdevancer_vsg_firmware					
Affected Version(s): * Up to (excluding) 1.11.00					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	9.8	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated attacker to execute an arbitrary OS command. **CVE ID : CVE-2023-22279**	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	17-Jan-2023	8.1	Cross-site request forgery (CSRF) vulnerability in MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in. **CVE ID : CVE-2023-22286**	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/578
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	7.2	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-22280**	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2023	6.1	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22296**	https://www.ate-mahoroba.jp/netdevancer/manual/	O-ATE-MAHO-030223/580
Vendor: Cisco					
Product: asyncos					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jan-2023	5.3	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. This vulnerability is due to improper processing of URLs. An attacker could exploit this vulnerability by crafting a URL in a particular	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh	O-CIS-ASYN-030223/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for an affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2023-20057**		
Product: ip_phones_8832_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/582
Product: ip_phone_7800_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/583
Product: ip_phone_7811_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_7821_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_7832_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/586
Product: ip_phone_7841_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-IP_P-030223/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	ityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	
Product: ip_phone_7861_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_8800_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/589
Product: ip_phone_8811_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/590
Product: ip_phone_8821-ex_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_8821_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_8831_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/593
Product: ip_phone_8832_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecur	O-CIS-IP_P-030223/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	ityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	
Product: ip_phone_8841_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_8845_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/596
Product: ip_phone_8851_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/597
Product: ip_phone_8861_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: ip_phone_8865_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-IP_P-030223/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			normally require authentication. **CVE ID : CVE-2023-20018**		
Product: roomos					
Affected Version(s): 10.11.3.0					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/600
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 10.11.5.2					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/603
Affected Version(s): 10.15.3.0					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/605
Affected Version(s): 10.3.2.0					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-ROOM-030223/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	roomos-dkjGFgRK	
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20002		
Affected Version(s): 10.3.4.0					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/608
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**		
Affected Version(s): 10.8.2.5					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/610
Server-Side Request	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/conte	O-CIS-ROOM-030223/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	nt/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	
Affected Version(s): 10.8.4.0					
N/A	20-Jan-2023	7.1	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to overwrite arbitrary files on the local system of an affected device. This vulnerability is due to improper access controls on files that are in the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to overwrite arbitrary files on the affected device. **CVE ID : CVE-2023-20008**		
Server-Side Request Forgery (SSRF)	20-Jan-2023	4.4	A vulnerability in Cisco TelePresence CE and RoomOS Software could allow an authenticated, local attacker to bypass access controls and conduct an SSRF attack through an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected system. **CVE ID : CVE-2023-20002**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK	O-CIS-ROOM-030223/613
Product: rv016_firmware					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	O-CIS-RV01-030223/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. **CVE ID : CVE-2023-20025**		
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	O-CIS-RV01-030223/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. **CVE ID : CVE-2023-20026**		
Product: rv042g_firmware					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. **CVE ID : CVE-2023-20025**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	O-CIS-RV04-030223/616
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/ci	O-CIS-RV04-030223/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. **CVE ID : CVE-2023-20026**	sco-sa-sbr042-multi-vuln-ej76Pke5	
Product: rv042_firmware					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	O-CIS-RV04-030223/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. **CVE ID : CVE-2023-20025**		
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	O-CIS-RV04-030223/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have valid Administrator credentials on the affected device. **CVE ID : CVE-2023-20026**		
Product: rv082_firmware					
Affected Version(s): -					
Improper Input Validation	20-Jan-2023	9.8	A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device. **CVE ID : CVE-2023-20025**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5	O-CIS-RV08-030223/620
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business Routers RV042 Series could allow an authenticated, remote attacker to inject	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-	O-CIS-RV08-030223/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on an affected device. This vulnerability is due to improper validation of user input fields within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device with root-level privileges. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. **CVE ID : CVE-2023-20026**	vuln-ej76Pke5	
Product: rv160w_wireless-ac_vpn_router_firmware					
Affected Version(s): * Up to (excluding) 1.0.01.04					
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-cmd-exe-n47kJQLE	O-CIS-RV16-030223/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator-level credentials on the affected device. **CVE ID : CVE-2023-20045**		
Product: rv160_vpn_router_firmware					
Affected Version(s): * Up to (excluding) 1.0.01.04					
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-cmd-exe-n47kJQLE	O-CIS-RV16-030223/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator-level credentials on the affected device. **CVE ID : CVE-2023-20045**		
Product: rv260p_vpn_router_with_poe_firmware					
Affected Version(s): * Up to (excluding) 1.0.01.04					
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-cmd-exe-n47kJQLE	O-CIS-RV26-030223/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary commands using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator-level credentials on the affected device. **CVE ID : CVE-2023-20045**		
Product: rv260_vpn_router_firmware					
Affected Version(s): * Up to (excluding) 1.0.01.04					
Improper Input Validation	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV160 and RV260 Series VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-cmd-exe-n47kJQLE	O-CIS-RV26-030223/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using root-level privileges on the affected device. To exploit this vulnerability, the attacker must have valid Administrator-level credentials on the affected device. **CVE ID : CVE-2023-20045**		
Product: rv340w_firmware					
Affected Version(s): * Up to (excluding) 1.0.03.29					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD	O-CIS-RV34-030223/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. **CVE ID : CVE-2023-20007**		
Product: rv340_firmware					
Affected Version(s): * Up to (excluding) 1.0.03.29					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD	O-CIS-RV34-030223/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. **CVE ID : CVE-2023-20007**		
Product: rv345p_firmware					
Affected Version(s): * Up to (excluding) 1.0.03.29					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based management interface. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD	O-CIS-RV34-030223/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. **CVE ID : CVE-2023-20007**		
Product: rv345_firmware					
Affected Version(s): * Up to (excluding) 1.0.03.29					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jan-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code or cause the web-based management process on the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The attacker must have valid administrator credentials. This vulnerability is due to insufficient validation of user-supplied input to the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rcedos-7HjP74jD	O-CIS-RV34-030223/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system or cause the web-based management process to restart, resulting in a DoS condition. **CVE ID : CVE-2023-20007**		
Product: unified_ip_phone_8851nr_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-UNIF-030223/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Product: unified_ip_phone_8865nr_firmware					
Affected Version(s): * Up to (excluding) 14.1\\(1\\)sr2					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-UNIF-030223/631
Product: webex_room_phone_firmware					
Affected Version(s): * Up to (including) 1.2.0					
Allocation of Resources	20-Jan-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature	https://sec.cloudapps.cisco.com/security	O-CIS-WEBE-030223/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. **CVE ID : CVE-2023-20047**	/center/content/CiscoSecurityAdvisory/cisco-sa-lldp-memlk-McOecPT	
Product: webex_share_firmware					
Affected Version(s): * Up to (including) 1.2.0					
Allocation of Resources	20-Jan-2023	6.5	A vulnerability in the Link Layer Discovery Protocol (LLDP) feature	https://sec.cloudapps.cisco.com/security	O-CIS-WEBE-030223/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			of Cisco Webex Room Phone and Cisco Webex Share devices could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient resource allocation. An attacker could exploit this vulnerability by sending crafted LLDP traffic to an affected device. A successful exploit could allow the attacker to exhaust the memory resources of the affected device, resulting in a crash of the LLDP process. If the affected device is configured to support LLDP only, this could cause an interruption to inbound and outbound calling. By default, these devices are configured to support both Cisco Discovery Protocol and LLDP. To recover operational state, the affected device needs a manual restart. **CVE ID : CVE-2023-20047**	/center/content/CiscoSecurityAdvisory/cisco-sa-lldp-memlk-McOecPT	
Product: wireless_ip_phone_8821-ex_firmware					
Affected Version(s): * Up to (excluding) 11.0\\(6\\)sr4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-WIRE-030223/634
Product: wireless_ip_phone_8821_firmware					
Affected Version(s): * Up to (excluding) 11.0\\(6\\)sr4					
Incorrect Authorization	20-Jan-2023	6.5	A vulnerability in the web-based management interface of Cisco IP Phone 7800 and 8800 Series Phones could allow an unauthenticated, remote attacker to bypass authentication on an affected device. This vulnerability is due to insufficient validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR	O-CIS-WIRE-030223/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to access certain parts of the web interface that would normally require authentication. **CVE ID : CVE-2023-20018**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
N/A	20-Jan-2023	9.8	Incorrect handling of '\0' bytes in file uploads in ModSecurity before 2.9.7 may allow for Web Application Firewall bypasses and buffer overflows on the Web Application Firewall when executing rules that read the FILES_TMP_CONTENT collection. **CVE ID : CVE-2023-24021**	https://github.com/SpiderLabs/ModSecurity/pull/2857/commits/4324f0ac59f8225aa44bc5034df60dbeccd1d334, https://github.com/SpiderLabs/ModSecurity/pull/2857	O-DEB-DEBI-030223/636
Improper Privilege Management	18-Jan-2023	7.8	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local	https://www.sudo.ws/security/advisories/sudoedit_any/, https://security.netapp.com/advisory/nta	O-DEB-DEBI-030223/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists because a user-specified editor may contain a "--" argument that defeats a protection mechanism, e.g., an EDITOR='vim --/path/to/extra/file' value. **CVE ID : CVE-2023-22809**	p-20230127-0015/	
Affected Version(s): 11.0					
Improper Privilege Management	18-Jan-2023	7.8	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists because a user-specified editor may contain a "--" argument that defeats a protection mechanism, e.g., an EDITOR='vim --	https://www.sudo.ws/security/advisories/sudoedit_any/, https://security.netapp.com/advisory/ntap-20230127-0015/	O-DEB-DEBI-030223/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/path/to/extra/file' value. **CVE ID : CVE-2023-22809**		
Vendor: Dell					
Product: powervault_me5012_firmware					
Affected Version(s): * Up to (excluding) me5.1.1.0.5					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. **CVE ID : CVE-2023-23691**	https://www.dell.com/support/kbdoc/en-us/000207533/dsa-2023-018-dell-emc-powervault-me5-security-update-for-a-client-desync-attack-vulnerability	O-DEL-POWE-030223/639
Product: powervault_me5024_firmware					
Affected Version(s): * Up to (excluding) me5.1.1.0.5					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS.	https://www.dell.com/support/kbdoc/en-us/000207533/dsa-2023-018-dell-emc-powervault-me5-security-update-for-a-client-desync-attack-vulnerability	O-DEL-POWE-030223/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23691		
Product: powervault_me5084_firmware					
Affected Version(s): * Up to (excluding) me5.1.1.0.5					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	20-Jan-2023	8.8	Dell EMC PV ME5, versions ME5.1.0.0.0 and ME5.1.0.1.0, contains a Client-side desync Vulnerability. An unauthenticated attacker could potentially exploit this vulnerability to force a victim's browser to desynchronize its connection with the website, typically leading to XSS and DoS. **CVE ID : CVE-2023-23691**	https://www.dell.com/support/kbdoc/en-us/000207533/dsa-2023-018-dell-emc-powervault-me5-security-update-for-a-client-desync-attack-vulnerability	O-DEL-POWE-030223/641
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 37					
Improper Privilege Management	18-Jan-2023	7.8	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p1. The problem exists	https://www.sudo.ws/security/advisories/sudoedit_any/, https://security.netapp.com/advisory/ntap-20230127-0015/	O-FED-FEDO-030223/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because a user-specified editor may contain a "--" argument that defeats a protection mechanism, e.g., an EDITOR='vim --/path/to/extra/file' value. **CVE ID : CVE-2023-22809**		
Vendor: Google					
Product: android					
Affected Version(s): -					
Use After Free	26-Jan-2023	7.8	In setUclampMinLocked of PowerSessionManager.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 kernelAndroid ID: A-236674672References: N/A **CVE ID : CVE-2023-20925**	https://source.android.com/security/bulletin/pixel/2023-01-01	O-GOO-ANDR-030223/643
Use After Free	26-Jan-2023	7.8	In binder_vma_close of binder.c, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254837884References: Upstream kernel **CVE ID : CVE-2023-20928**		
Improper Authentication	26-Jan-2023	6.8	In (TBD) of (TBD), there is a possible way to bypass the lockscreen due to Biometric Auth Failure. This could lead to local escalation of privilege with physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-240428519References: N/A **CVE ID : CVE-2023-20924**	https://source.android.com/security/bulletin/pixel/2023-01-01	O-GOO-ANDR-030223/645
N/A	26-Jan-2023	5.5	In exported content providers of ShannonRcs, there is a possible way to get access to protected content providers due to a permissions bypass. This could lead to local information disclosure with no additional execution	https://source.android.com/security/bulletin/pixel/2023-01-01	O-GOO-ANDR-030223/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-246933910References: N/A **CVE ID : CVE-2023-20923**		
Affected Version(s): 10.0					
Out-of-bounds Write	26-Jan-2023	7.8	In Mfc_Transceive 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-241387741 **CVE ID : CVE-2023-20905**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/647
Always-Incorrect Control Flow Implementation	26-Jan-2023	7.8	In addOrReplacePhoneAccount of PhoneAccountRegistrar.java, there is a possible way to enable a phone account without user interaction due to a logic error in the code. This could lead to local escalation of privilege with no additional	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-246930197 **CVE ID : CVE-2023-20915**		
Use After Free	26-Jan-2023	7.8	In queue of UsbRequest.java, 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-204584366 **CVE ID : CVE-2023-20920**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/649
Always-Incorrect Control Flow Implementation	26-Jan-2023	7.3	In onPackageRemoved of AccessibilityManagerService.java, there is a possibility to automatically grant accessibility services due to a logic error in the code. This could	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-243378132 **CVE ID : CVE-2023-20921**		
Uncontrolled Resource Consumption	26-Jan-2023	5.5	In several functions of SettingsState.java, there is a possible system crash loop due to resource exhaustion. This could lead to local denial of service 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-239415861 **CVE ID : CVE-2023-20908**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/651
Affected Version(s): 11.0					
Always-Incorrect Control Flow Implementation	26-Jan-2023	7.8	In addOrReplacePhoneAccount of PhoneAccountRegistrar.java, there is a possible way to enable a phone	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account without user interaction due to a logic error in the code. 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-246930197 **CVE ID : CVE-2023-20915**		
Use After Free	26-Jan-2023	7.8	In queue of UsbRequest.java, 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-204584366 **CVE ID : CVE-2023-20920**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Always-Incorrect Control Flow Implementation	26-Jan-2023	7.3	In onPackageRemoved of AccessibilityManagerService.java, there is a possibility to automatically grant accessibility services due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-243378132 **CVE ID : CVE-2023-20921**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/654
Uncontrolled Resource Consumption	26-Jan-2023	5.5	In several functions of SettingsState.java, there is a possible system crash loop due to resource exhaustion. This could lead to local denial of service 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-239415861	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20908		
Uncontrolled Resource Consumption	26-Jan-2023	5.5	In setMimeGroup of PackageManagerService.java, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service 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-237291548 **CVE ID : CVE-2023-20922**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/656
Affected Version(s): 12.0					
Always-Incorrect Control Flow Implementation	26-Jan-2023	7.8	In addOrReplacePhoneAccount of PhoneAccountRegistrar.java, there is a possible way to enable a phone account without user interaction due to a logic error in the code. 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-	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A-246930197 **CVE ID : CVE-2023-20915**		
Missing Authorization	26-Jan-2023	7.8	In getMainActivityLaunchIntent of LauncherAppsService.java, there is a possible way to bypass the restrictions on starting activities from the background due to a missing permission 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-12 Android-12LAndroid ID: A-229256049 **CVE ID : CVE-2023-20916**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/658
Use After Free	26-Jan-2023	7.8	In queue of UsbRequest.java, 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	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12 Android-12L Android-13Android ID: A-204584366 **CVE ID : CVE-2023-20920**		
Always-Incorrect Control Flow Implementation	26-Jan-2023	7.3	In onPackageRemoved of AccessibilityManagerService.java, there is a possibility to automatically grant accessibility services due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-243378132 **CVE ID : CVE-2023-20921**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/660
Uncontrolled Resource Consumption	26-Jan-2023	5.5	In several functions of SettingsState.java, there is a possible system crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239415861 **CVE ID : CVE-2023-20908**		
Uncontrolled Resource Consumption	26-Jan-2023	5.5	In setMimeGroup of PackageManagerService.java, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service 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-237291548 **CVE ID : CVE-2023-20922**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/662
Affected Version(s): 12.1					
N/A	26-Jan-2023	7.8	In getTrampolineIntent of SettingsActivity.java, there is a possible launch of arbitrary activity due to an Intent mismatch in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12L Android-13Android ID: A-246300272 **CVE ID : CVE-2023-20904**		
Always-Incorrect Control Flow Implementation	26-Jan-2023	7.8	In addOrReplacePhoneAccount of PhoneAccountRegistrar.java, there is a possible way to enable a phone account without user interaction due to a logic error in the code. 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-246930197 **CVE ID : CVE-2023-20915**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/664
Missing Authorization	26-Jan-2023	7.8	In getMainActivityLaunchIntent of LauncherAppsService.java, there is a possible way to bypass the restrictions on starting activities from the background due to a missing permission check. This could lead to local escalation of privilege with no	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-229256049 **CVE ID : CVE-2023-20916**		
Use After Free	26-Jan-2023	7.8	In queue of UsbRequest.java, 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-204584366 **CVE ID : CVE-2023-20920**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/666
Always-Incorrect Control Flow Implementation	26-Jan-2023	7.3	In onPackageRemoved of AccessibilityManagerService.java, there is a possibility to automatically grant accessibility services due to a logic error in the code. This could lead to local escalation of privilege with no	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-243378132 **CVE ID : CVE-2023-20921**		
Uncontrolled Resource Consumption	26-Jan-2023	5.5	In several functions of SettingsState.java, there is a possible system crash loop due to resource exhaustion. This could lead to local denial of service 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-239415861 **CVE ID : CVE-2023-20908**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/668
Uncontrolled Resource Consumption	26-Jan-2023	5.5	In setMimeGroup of PackageManagerService.java, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-237291548 **CVE ID : CVE-2023-20922**		
Affected Version(s): 13.0					
N/A	26-Jan-2023	7.8	In getTrampolineIntent of SettingsActivity.java, there is a possible launch of arbitrary activity due to an Intent mismatch in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-246300272 **CVE ID : CVE-2023-20904**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/670
Always-Incorrect Control Flow Implementation	26-Jan-2023	7.8	In addOrReplacePhoneAccount of PhoneAccountRegistrar.java, there is a possible way to enable a phone account without user interaction due to a logic error in the code. This could lead to local escalation of privilege with no additional	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-246930197 **CVE ID : CVE-2023-20915**		
N/A	26-Jan-2023	7.8	In getStringsForPrefix of Settings.java, there is a possible prevention of package uninstallation due to a logic error in the code. 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-252663068 **CVE ID : CVE-2023-20919**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/672
Use After Free	26-Jan-2023	7.8	In queue of UsbRequest.java, 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	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/673

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-204584366 **CVE ID : CVE-2023-20920**		
Always-Incorrect Control Flow Implementation	26-Jan-2023	7.3	In onPackageRemoved of AccessibilityManagerService.java, there is a possibility to automatically grant accessibility services due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-243378132 **CVE ID : CVE-2023-20921**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/674
Uncontrolled Resource Consumption	26-Jan-2023	5.5	In several functions of SettingsState.java, there is a possible system crash loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239415861 **CVE ID : CVE-2023-20908**		
Uncontrolled Resource Consumption	26-Jan-2023	5.5	In setMimeGroup of PackageManagerService.java, there is a possible crash loop due to resource exhaustion. This could lead to local denial of service 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-237291548 **CVE ID : CVE-2023-20922**	https://source.android.com/security/bulletin/2023-01-01	O-GOO-ANDR-030223/676
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Exposure of Sensitive Information to an Unauthorized Actor	17-Jan-2023	7.5	IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that	https://exchange.xforce.ibmcloud.com/vulnerabilities/244356, https://www.ibm.com/support/pages/node/6855643	O-LIN-LINU-030223/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key. IBM X-Force ID: 244356. **CVE ID : CVE-2023-22875**		
Affected Version(s): * Up to (excluding) 6.1					
Use After Free	26-Jan-2023	5.5	A use-after-free flaw was found in io_uring/filetable.c in io_install_fixed_file in the io_uring subcomponent in the Linux Kernel during call cleanup. This flaw may lead to a denial of service. **CVE ID : CVE-2023-0469**	https://bugzilla.redhat.com/show_bug.cgi?id=2163723	O-LIN-LINU-030223/678
Use After Free	26-Jan-2023	4.7	A use-after-free flaw was found in io_uring/poll.c in io_poll_check_events in the io_uring subcomponent in the Linux Kernel due to a race condition of poll_refs. This flaw may cause a NULL pointer dereference. **CVE ID : CVE-2023-0468**	https://bugzilla.redhat.com/show_bug.cgi?id=2164024	O-LIN-LINU-030223/679
Affected Version(s): * Up to (excluding) 6.2					
NULL Pointer Dereference	26-Jan-2023	5.5	A NULL pointer dereference flaw was found in rawv6_push_pending_frames in net/ipv6/raw.c in the network subcomponent in the Linux kernel. This flaw causes the system to crash.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=cb3e9864cdbe35ff6378966660edbcbac955fe17	O-LIN-LINU-030223/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0394		
Affected Version(s): 6.0					
NULL Pointer Dereference	17-Jan-2023	7.5	A NULL pointer dereference vulnerability in the Linux kernel NVMe functionality, in nvmet_setup_auth(), allows an attacker to perform a Pre-Auth Denial of Service (DoS) attack on a remote machine. Affected versions v6.0-rc1 to v6.0-rc3, fixed in v6.0-rc4. **CVE ID : CVE-2023-0122**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=da0342a3aa0357795224e6283df86444e1117168	O-LIN-LINU-030223/681
Affected Version(s): 6.1					
Use After Free	26-Jan-2023	5.5	A use-after-free flaw was found in io_uring/filetable.c in io_install_fixed_file in the io_uring subcomponent in the Linux Kernel during call cleanup. This flaw may lead to a denial of service. **CVE ID : CVE-2023-0469**	https://bugzilla.redhat.com/show_bug.cgi?id=2163723	O-LIN-LINU-030223/682
Use After Free	26-Jan-2023	4.7	A use-after-free flaw was found in io_uring/poll.c in io_poll_check_events in the io_uring subcomponent in the Linux Kernel due to a race condition of poll_refs. This flaw may	https://bugzilla.redhat.com/show_bug.cgi?id=2164024	O-LIN-LINU-030223/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a NULL pointer dereference. **CVE ID : CVE-2023-0468**		
Affected Version(s): 6.2					
NULL Pointer Dereference	26-Jan-2023	5.5	A NULL pointer dereference flaw was found in rawv6_push_pending_frames in net/ipv6/raw.c in the network subcomponent in the Linux kernel. This flaw causes the system to crash. **CVE ID : CVE-2023-0394**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=cb3e9864cdbe35ff6378966660edbcbac955fe17	O-LIN-LINU-030223/684
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Integer Overflow or Wraparound	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by an Integer Overflow or Wraparound 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-2023-21579**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21604**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/686
Heap-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21605**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21606**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/688
Improper Input Validation	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21607**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/689
Use After Free	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and	https://helpx.adobe.com/security/produc	O-MIC-WIND-030223/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 20.005.30418 (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-2023-21608**	ts/acrobat/apsb23-01.html	
Out-of-bounds Write	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21609**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/691
Stack-based Buffer Overflow	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Stack-based Buffer Overflow vulnerability	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-21610**		
Exposure of Resource to Wrong Sphere	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21611**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/693
Creation of Temporary File in Directory with Insecure Permissions	18-Jan-2023	7.8	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (and earlier) are affected by a Creation of Temporary File in Directory with	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Incorrect Permissions vulnerability that could result in privilege escalation 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-2023-21612**		
Cleartext Transmission of Sensitive Information	18-Jan-2023	5.9	IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitly specified in the URL. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 244109. **CVE ID : CVE-2023-22863**	https://www.ibm.com/support/pages/node/6855837, https://exchange.xforce.ibmcloud.com/vulnerabilities/244109	O-MIC-WIND-030223/695
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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/acrobat/apsb23-01.html	O-MIC-WIND-030223/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-21581**		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21585**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/697
Use After Free	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (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.	https://helpx.adobe.com/security/products/dimension/apsb23-10.html	O-MIC-WIND-030223/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21601		
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Dimension version 3.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-21603**	https://helpx.adobe.com/security/products/dimension/apsb23-10.html	O-MIC-WIND-030223/699
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21613**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2023	5.5	Adobe Acrobat Reader versions 22.003.20282 (and earlier), 22.003.20281 (and earlier) and 20.005.30418 (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-2023-21614**	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html	O-MIC-WIND-030223/701
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	5.4	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 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: 244075. **CVE ID : CVE-2023-22594**	https://www.ibm.com/support/pages/node/6855835, https://exchange.xforce.ibmcloud.com/vulnerabilities/244075	O-MIC-WIND-030223/702
Vendor: Omron					
Product: cp1l-el20dr-d_firmware					
Affected Version(s): *					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Jan-2023	9.8	Active debug code exists in OMRON CP1L-EL20DR-D all versions, which may lead to a command that is not specified in FINS protocol being executed without authentication. A remote unauthenticated attacker may read/write in arbitrary area of the device memory, which may lead to overwriting the firmware, causing a denial-of-service (DoS) condition, and/or arbitrary code execution. **CVE ID : CVE-2023-22357**	N/A	O-OMR-CP1L-030223/703
Product: cx-motion-mch_firmware					
Affected Version(s): * Up to (excluding) 2.33					
Access of Uninitialized Pointer	17-Jan-2023	7.8	CX-Motion-MCH v2.32 and earlier contains an access of uninitialized pointer vulnerability. Having a user to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution. **CVE ID : CVE-2023-22366**	N/A	O-OMR-CX-M-030223/704
Vendor: Oracle					
Product: solaris					
Affected Version(s): 10					
N/A	18-Jan-2023	4	Vulnerability in the Oracle Solaris product	https://www.oracle.com/se	O-ORA-SOLA-030223/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Oracle Systems (component: NSSwitch). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 4.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:N/I:L/A:L). **CVE ID : CVE-2023-21900**	curity-alerts/cpujan2023.html	
Affected Version(s): 11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2023	4	Vulnerability in the Oracle Solaris product of Oracle Systems (component: NSSwitch). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 4.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:N/I:L/A:L).	https://www.oracle.com/security-alerts/cpujan2023.html	O-ORA-SOLA-030223/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21900		
Vendor: pixela					
Product: pix-rt100_firmware					
Affected Version(s): 2.1.1_eq101					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jan-2023	8	OS command injection vulnerability in PIX-RT100 versions RT100_TEQ_2.1.1_EQ101 and RT100_TEQ_2.1.2_EQ101 allows a network-adjacent attacker who can access product settings to execute an arbitrary OS command. **CVE ID : CVE-2023-22304**	https://www.pixela.co.jp/products/network/pix_rt100/update.html	O-PIX-PIX--030223/707
N/A	17-Jan-2023	6.5	Hidden functionality vulnerability in PIX-RT100 versions RT100_TEQ_2.1.1_EQ101 and RT100_TEQ_2.1.2_EQ101 allows a network-adjacent attacker to access the product via undocumented Telnet or SSH services. **CVE ID : CVE-2023-22316**	https://www.pixela.co.jp/products/network/pix_rt100/update.html	O-PIX-PIX--030223/708
Affected Version(s): 2.1.2_eq101					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jan-2023	8	OS command injection vulnerability in PIX-RT100 versions RT100_TEQ_2.1.1_EQ101 and RT100_TEQ_2.1.2_EQ101 allows a network-adjacent attacker who can access product	https://www.pixela.co.jp/products/network/pix_rt100/update.html	O-PIX-PIX--030223/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			settings to execute an arbitrary OS command. **CVE ID : CVE-2023-22304**		
N/A	17-Jan-2023	6.5	Hidden functionality vulnerability in PIX-RT100 versions RT100_TEQ_2.1.1_EQ101 and RT100_TEQ_2.1.2_EQ101 allows a network-adjacent attacker to access the product via undocumented Telnet or SSH services. **CVE ID : CVE-2023-22316**	https://www.pixela.co.jp/products/network/pix_rt100/update.html	O-PIX-PIX--030223/710
Vendor: Redhat					
Product: openshift					
Affected Version(s): -					
Incorrect Permission Assignment for Critical Resource	18-Jan-2023	7.8	IBM Robotic Process Automation for Cloud Pak 21.0.1 through 21.0.4 could allow a local user to perform unauthorized actions due to insufficient permission settings. IBM X-Force ID: 244073. **CVE ID : CVE-2023-22592**	https://www.ibm.com/support/pages/node/6855839, https://exchange.xforce.ibmcloud.com/vulnerabilities/244073	O-RED-OPEN-030223/711
Cleartext Transmission of Sensitive Information	18-Jan-2023	5.9	IBM Robotic Process Automation 20.12.0 through 21.0.2 defaults to HTTP in some RPA commands when the prefix is not explicitly specified in the URL. This could allow an attacker to obtain	https://www.ibm.com/support/pages/node/6855837, https://exchange.xforce.ibmcloud.com/vulnerabilities/244109	O-RED-OPEN-030223/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information using man in the middle techniques. IBM X-Force ID: 244109. **CVE ID : CVE-2023-22863**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2023	5.4	IBM Robotic Process Automation for Cloud Pak 20.12.0 through 21.0.4 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: 244075. **CVE ID : CVE-2023-22594**	https://www.ibm.com/support/pages/node/6855835, https://exchange.xforce.ibmcloud.com/vulnerabilities/244075	O-RED-OPEN-030223/713
Vendor: Sonicwall					
Product: sma1000_firmware					
Affected Version(s): 12.4.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Jan-2023	7.5	Pre-authentication path traversal vulnerability in SMA1000 firmware version 12.4.2, which allows an unauthenticated attacker to access arbitrary files and directories stored outside the web root directory. **CVE ID : CVE-2023-0126**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0001	O-SON-SMA1-030223/714
Vendor: Tenda					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ac18_firmware					
Affected Version(s): 15.03.05.19					
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/FUN_000c2318. **CVE ID : CVE-2023-24164**	N/A	O-TEN-AC18-030223/715
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/initIpAddrInfo. **CVE ID : CVE-2023-24165**	N/A	O-TEN-AC18-030223/716
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/formWifiBasicSet. **CVE ID : CVE-2023-24166**	N/A	O-TEN-AC18-030223/717
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/add_white_node. **CVE ID : CVE-2023-24167**	N/A	O-TEN-AC18-030223/718
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/FUN_0007343c.	N/A	O-TEN-AC18-030223/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24169		
Out-of-bounds Write	26-Jan-2023	9.8	Tenda AC18 V15.03.05.19 is vulnerable to Buffer Overflow via /goform/fromSetWirelessRepeat. **CVE ID : CVE-2023-24170**	N/A	O-TEN-AC18-030223/720
Vendor: Tp-link					
Product: tl-sg105pe_firmware					
Affected Version(s): 1.0.0					
Improper Authentication	17-Jan-2023	9.8	TP-Link SG105PE firmware prior to 'TL-SG105PE(UN) 1.0_1.0.0 Build 20221208' contains an authentication bypass vulnerability. Under the certain conditions, an attacker may impersonate an administrator of the product. As a result, information may be obtained and/or the product's settings may be altered with the privilege of the administrator. **CVE ID : CVE-2023-22303**	https://www.tp-link.com/jp/support/download/tl-sg105pe/v1/#Firmware, https://www.tp-link.com/en/business-networking/easy-smart-switch/tl-sg105pe/	O-TP--TL-S-030223/721
Vendor: Trendnet					
Product: tew-820ap_firmware					
Affected Version(s): 1.01.b01					
Out-of-bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-	N/A	O-TRE-TEW--030223/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formSystemCheck. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-24095**		
Out-of-bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the newpass parameter at /formPasswordSetup. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-24096**	N/A	O-TRE-TEW--030223/723
Out-of-bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware	N/A	O-TRE-TEW--030223/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formPasswordAuth. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-24097**		
Out-of-bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a stack overflow via the submit-url parameter at /formSysLog. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-24098**	N/A	O-TRE-TEW--030223/725
Out-of-bounds Write	23-Jan-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** TrendNet Wireless AC Easy-Upgrader TEW-820AP v1.0R, firmware version 1.01.B01 was discovered to contain a	N/A	O-TRE-TEW--030223/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack overflow via the username parameter at /formWizardPassword. This vulnerability allows attackers to execute arbitrary code via a crafted payload. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-24099**		
Vendor: zephyrproject					
Product: zephyr					
Affected Version(s): * Up to (including) 3.2.0					
Improper Initialization	19-Jan-2023	6.5	A malicious / defect bluetooth controller can cause a Denial of Service due to unchecked input in le_read_buffer_size_complete. **CVE ID : CVE-2023-0397**	N/A	O-ZEP-ZEPH-030223/727